(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2003－516000
（P2003－516000A）
(43)公表日　平成15年５月７日(2003.5.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｑ　7/38		Ｈ０４Ｌ　12/28	３１０	５Ｋ０３３
Ｈ０４Ｌ　12/28	３１０	Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０６７
Ｈ０４Ｑ　7/22			１０７	

審査請求　未請求　予備審査請求　有　（全 48 頁）

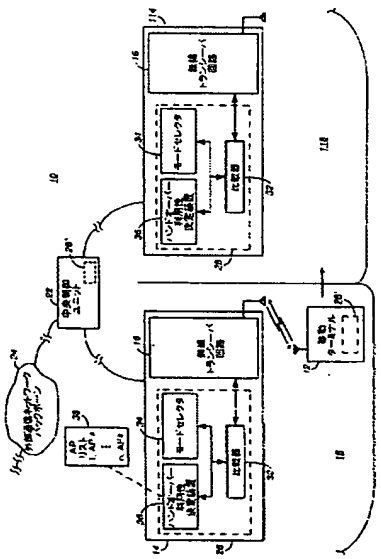
(21)出願番号　特願2001－540557(P2001－540557)
(86)(22)出願日　平成12年11月21日(2000.11.21)
(85)翻訳文提出日　平成14年５月23日(2002.5.23)
(86)国際出願番号　ＰＣＴ／ＩＢ００／０１７１３
(87)国際公開番号　ＷＯ０１／０３９５３８
(87)国際公開日　平成13年５月31日(2001.5.31)
(31)優先権主張番号　０９／４４７，７６１
(32)優先日　平成11年11月23日(1999.11.23)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ノキア　コーポレイション
フィンランド　エフイーエン－02150　エスプー　ケイララーデンティエ　４
(72)発明者　アラーラウリラ　ユハ
フィンランド　エフイーエン－33210　タンペレ　ムスタンラーデンカトゥ　10アー５
(72)発明者　ハンセン　ハリ
フィンランド　エフイーエン－02200　エスプー　ノキトンテュンクヤ　１エー34
(74)代理人　弁理士　中村　稔　（外９名）

最終頁に続く

(54)【発明の名称】　移動ターミナルハンドオーバー中のセキュリティ関連性の転送

(57)【要約】
ＩＥＥＥ８０２．１１又はＨＩＰＥＲＬＡＮのような無線通信システムにおいて通信ハンドオーバー事象が発生したときに既存のセキュリティ関連性が再確立され、ワイヤレス通信ネットワーク内で通信ハンドオーバーが生じたときに移動ターミナルとそのネットワークとの間の既存のセキュリティ関連性が維持される。ハンドオーバー事象中の認証は、チャレンジ／応答手順によって達成される。このチャレンジ／応答手順によれば、新たなアクセスポイントと、この新たなアクセスポイントへのハンドオーバーを経験する移動ターミナルとで形成された通信対の各メンバーは、その通信対の他のメンバーへチャレンジを送信する。通信対の各メンバーは、次いで、その受信したチャレンジに対する応答を計算し、これら応答は、通信対の他のメンバーへ返送される。通信対の各メンバーは、次いで、その受信した応答を正しい応答と比較する。これら比較が正しいときには、第２アクセスポイントと移動ターミナルとの間でペイロード通信が開始される。



【特許請求の範囲】

【請求項１】 所定の移動ターミナルとの通信が第１アクセスポイントから第２アクセスポイントへハンドオーバーされるときに情報セキュリティを与える方法において、

複数のアクセスポイントを有する通信システムを用意し、各アクセスポイントは、上記通信システムによりサービスされる全地理的エリア内の異なる地理的エリアにサービスし、

上記全地理的エリア内で上記異なる地理的エリア間を各々物理的に移動可能な複数の移動ターミナルを用意し、

上記所定の移動ターミナルが上記第１アクセスポイントとの通信作用から上記第２アクセスポイントとの通信作用へ移動するときを感知し、

上記感知段階に応答して、上記第１アクセスポイントからセキュリティ関連性パラメータを検索し、その検索されたセキュリティ関連性パラメータに基づいて上記第２アクセスポイントにセキュリティ関連性を形成し、そしてその検索されたセキュリティ関連性パラメータに基づいて上記所定の移動ターミナルにセキュリティ関連性を形成し、そして

上記第１比較段階及び上記第２比較段階に基づいて上記所定の移動ターミナルと上記第２アクセスポイントとの間に通信を開始する、

という段階を備えた方法。

【請求項２】 上記の感知段階に応答して、上記所定の移動ターミナルから上記第２アクセスポイントへ認証アクセスポイントチャレンジを送信し、そして上記第２アクセスポイントから上記所定の移動ターミナルへ認証移動ターミナルチャレンジを送信し、

上記所定の移動ターミナルから受け取った上記認証アクセスポイントチャレンジに応答して上記第２アクセスポイントに認証アクセスポイント応答を発生し、

上記認証アクセスポイント応答を上記所定の移動ターミナルへ送信し、

上記第２アクセスポイントから受け取った上記認証移動ターミナルチャレンジに応答して上記所定の移動ターミナルに認証移動ターミナル応答を発生し、

上記認証移動ターミナル応答を上記第２アクセスポイントへ送信し、

上記認証アクセスポイント応答を上記所定の移動ターミナルにおいて正しい応答と第１比較し、

上記認証移動ターミナル応答を上記第２アクセスポイントにおいて正しい応答と第２比較し、そして

上記第１比較段階及び上記第２比較段階に基づいて上記所定の移動ターミナルと上記第２アクセスポイントとの間に通信を開始する、

段階を更に備えた請求項１に記載の方法。

【請求項３】　上記複数の移動ターミナルは、媒体アクセス制御層及び互換性物理層を有し、そして上記メッセージは、媒体アクセス制御メッセージである請求項２に記載の方法。

【請求項４】　上記メッセージは、ＩＥＥＥ８０２．１１のようなワイヤレスＬＡＮ内に送信されるか、又はＨＩＰＥＲＬＡＮ／２マルチアクセスメッセージである請求項３に記載の方法。

【請求項５】　上記通信システムは、セキュリティプロトコルを使用してデータパケットの端－端セキュリティを与えるＷＬＡＮ通信システムである請求項２に記載の方法。

【請求項６】　上記端－端セキュリティは、上記データパケットを認証及び／又は暗号化することにより与えられ、そして上記セキュリティプロトコルは、通信リンクの両端で同じ暗号及び／又は認証キーの使用を必要とする対称的暗号を与える請求項５に記載の方法。

【請求項７】　シール可能なキー管理プロトコルは、上記セキュリティプロトコルに対する対称的キーを発生するように動作する請求項６に記載の方法。

【請求項８】　上記所定の移動ターミナルと上記第２のアクセスポイントとの間にセッション従属動的暗号化キーを与え、そして

上記通信システムにより与えられる通信カバレージ内で上記所定の移動ターミナルが移動するときに第１アクセスポイントから第２アクセスポイントへアクティブなセキュリティ関連性を転送する、

という段階を備えた請求項６に記載の方法。

【請求項９】　上記通信システムをＬＡＮとして用意し、

上記ＬＡＮ内にサーバーを用意し、

通信ハンドオーバー中に通信が続くときに、端－端セキュリティ関連性に変更を必要とせずに、通信ハンドオーバー中に上記ＬＡＮ内にキー管理及びセキュリティ関連性再確立を与え、上記通信ハンドオーバーが上記移動ターミナルと上記第１及び第２アクセスポイントとの間のセキュリティ機能にしか影響しないようにする、

という段階を備えた請求項４に記載の方法。

【請求項１０】　上記ＬＡＮは、上記複数のアクセスポイントと上記複数の移動ターミナルとの間にインターネットプロトコルセキュリティベースのセキュリティ関連性を含む請求項９に記載の方法。

【請求項１１】　上記所定の移動ターミナル及び上記第１及び第２のアクセスポイントで作られた通信対の両端に対して認証キーが与えられ、この認証キーは、スケーリング可能なキー管理プロトコルにより発生される請求項１に記載の方法。

【請求項１２】　上記所定の移動ターミナルと上記第１アクセスポイントとの間にはスケーリング可能なキー管理プロトコルに基づいて認証キー又はセキュリティ関連性が存在し、そして通信ハンドオーバー中に新たなキー交換の必要性を回避するために上記複数のアクセスポイント間にセキュリティ関連性が転送される請求項１に記載の方法。

【請求項１３】　上記シール可能なキー管理プロトコルは、ＩＫＥであり、そして上記第１アクセスポイントから上記第２アクセスポイントへの上記通信ハンドオーバー中に新たなキー交換の必要性を回避するやり方で上記第１アクセスポイントと上記第２アクセスポイントとの間にセキュリティ関連性が転送される請求項１２に記載の方法。

【請求項１４】　キーを搬送するメッセージを暗号化する段階を含む請求項１３に記載の方法。

【請求項１５】　無線通信システムに通信ハンドオーバー事象が生じるときにセキュリティ関連性を維持するためのチャレンジ／応答方法において、

アクセスポイントと、このアクセスポイントへの通信ハンドオーバーを経験す

る移動ターミナルとで作られた通信対を用意し、

上記移動ターミナルから上記アクセスポイントへ第１チャレンジを送信し、

上記アクセスポイントから上記移動ターミナルへ第２チャレンジを送信し、

上記アクセスポイントにおいて上記受信した第１チャレンジに対する第１応答を計算し、

上記移動ターミナルへ上記第１応答を送信し、

上記移動ターミナルにおいて上記受信した第２チャレンジに対する第２応答を計算し、

上記アクセスポイントへ上記第２応答を送信し、

上記受信された第１応答を上記移動ターミナルにおいて正しい応答と第１比較し、

上記受信された第２応答を上記アクセスポイントにおいて正しい応答と第２比較し、そして

上記第１比較段階及び第２比較段階に基づき上記アクセスポイントと上記移動ターミナルとの間で通信を開始する、

という段階を備えた方法。

【請求項１６】　上記無線通信システムは、グループＩＥＥＥ８０２．１１及びＨＩＰＥＲＬＡＮから選択される請求項１５に記載の方法。

【請求項１７】　上記移動ターミナルは、上記通信ハンドオーバー事象の前に別のアクセスポイントと通信状態にあり、そして上記セキュリティ関連性は、上記移動ターミナルと上記別のアクセスポイントとの間に存在するセキュリティ関連性である請求項１５に記載の方法。

【請求項１８】　第１通信アクセスポイントによりサービスされる第１地理的エリアから、第２通信アクセスポイントによりサービスされる第２地理的エリアへ移動ターミナルが物理的に移動するときに通信ハンドオーバーが発生するとき無線通信システムに所定のセキュリティ関連性を維持するための装置であって、上記移動ターミナルは、最初に、上記第１通信アクセスポイントと第１通信対を形成し、そして上記通信ハンドオーバーの後に、上記移動ターミナルは、上記第２通信アクセスポイントと第２通信対を形成し、上記第１通信対の各メンバー

は、それに関連した上記所定のセキュリティ関連性を有し、上記装置は、

上記移動ターミナルにあって上記通信ハンドオーバーを開始する必要性を感知するための第１手段と、

上記無線通信システム内にあって、上記第１手段が上記通信ハンドオーバーを開始する上記必要性を感知するのに応答して、上記第２通信アクセスポイントに上記所定のセキュリティ関連性を確立するための第２手段と、

上記移動ターミナルにあって、上記所定のセキュリティ関連性の関数としてアクセスポイントチャレンジを発生し、そしてそのアクセスポイントチャレンジを上記第２通信アクセスポイントへ送信するための第３手段と、

上記第２通信アクセスポイントにあって、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として移動ターミナルチャレンジを発生し、そしてその移動ターミナルチャレンジを上記移動ターミナルへ送信するための第４手段と、

上記移動ターミナルにあって、上記移動ターミナルチャレンジに応答して、上記所定のセキュリティ関連性の関数として移動ターミナル応答を発生し、そしてその移動ターミナル応答を上記第２通信アクセスポイントへ送信するための第５手段と、

上記第２通信アクセスポイントにあって、上記アクセスポイントチャレンジに応答して、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数としてアクセスポイント応答を発生し、そしてそのアクセスポイント応答を上記移動ターミナルへ送信するための第６手段と、

上記移動ターミナルにあって、上記アクセスポイント応答に応答して、上記アクセスポイント応答が上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第７手段と、

上記第２通信アクセスポイントにあって、上記移動ターミナル応答に応答して、上記移動ターミナル応答が、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第８手段と、

上記無線通信システムにあって、上記第８及び第９手段に応答して、上記移動

ターミナル応答及び上記アクセスポイント応答の両方が正しいときに上記通信ハンドオーバーを確立するための第９手段と、

を備えた装置。

【請求項１９】　上記無線通信システムは、グループＩＥＥＥ８０２．１１及びＨＩＰＥＲＬＡＮから選択される請求項１８に記載の装置。

【請求項２０】　移動ターミナルの通信ハンドオーバーが発生するとき無線通信システムに所定のセキュリティ関連性を維持するための方法であって、上記移動ターミナルは、最初に、第１通信アクセスポイントと第１通信対を形成し、そして上記通信ハンドオーバーの後に、上記移動ターミナルは、第２通信アクセスポイントと第２通信対を形成し、上記第１通信対の各メンバーは、それに関連した上記所定のセキュリティ関連性を有し、上記方法は、

上記通信ハンドオーバーを開始する必要性を感知し、

上記通信ハンドオーバーを開始する上記必要性に応答し、そしてそれに応答して上記第２通信アクセスポイントに上記所定のセキュリティ関連性を確立し、

上記移動ターミナルに、上記所定のセキュリティ関連性の関数としてアクセスポイントチャレンジを発生し、

そのアクセスポイントチャレンジを上記第２通信アクセスポイントへ送信し、

上記第２通信アクセスポイントに、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として移動ターミナルチャレンジを発生し、

その移動ターミナルチャレンジを上記移動ターミナルへ送信し、

上記移動ターミナルにおいて上記移動ターミナルチャレンジに応答して、上記所定のセキュリティ関連性の関数として移動ターミナル応答を発生し、

その移動ターミナル応答を上記第２通信アクセスポイントへ送信し、

上記第２通信アクセスポイントにおいて上記アクセスポイントチャレンジに応答して、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数としてアクセスポイント応答を発生し、

そのアクセスポイント応答を上記移動ターミナルへ送信し、

上記移動ターミナルにおいて上記アクセスポイント応答に応答して、上記アク

セスポイント応答が上記所定のセキュリティ関連性の関数として正しいかどうか決定し、

上記第２通信アクセスポイントにおいて上記移動ターミナル応答に応答して、上記移動ターミナル応答が、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として正しいかどうか決定し、そして

上記移動ターミナル応答及び上記アクセスポイント応答の両方が正しいときに上記通信ハンドオーバーを確立する、

という段階を備えた方法。

【発明の詳細な説明】

【０００１】

【技術分野】

本発明は、ワイヤレスレスローカルエリアネットワーク（ＷＬＡＮ）が非限定例である無線通信システムに係る。より詳細には、本発明は、移動ターミナルが第１ベースステーション又はアクセスポイント（ＡＰ）から第２ベースステーション又はアクセスポイント（ＡＰ）へハンドオーバーされるときに情報セキュリティを与えることに係る。

【０００２】

【背景技術】

最小限の構成においては、通信システムが送信ステーション及び受信ステーションで形成され、それらが通信チャンネルにより相互接続される。送信ステーションにより発生された通信信号は、通信チャンネルに送信され、そして受信ステーションにより受信される。

無線通信システムでは、通信チャンネルの少なくとも一部分が電磁スペクトルの一部分によって形成される。無線通信システムでは、送信ステーションと受信ステーションとの間に固定接続やハード布線接続が要求されないので、通信移動度を高めることができる。

【０００３】

セルラー電話システムが一例であるセルラー通信システムは、無線通信システムの一例である。セルラー通信システムに対する加入者の移動ターミナルが、セルラー通信システムのネットワークインフラストラクチャーによって包囲されたエリア全体にわたりせいぜいどこかの位置に物理的に配置されるだけであるときには、移動ターミナルは、セルラー通信システムによって別の移動ターミナルと通信することができる。

例示的なワイヤレス通信システムのネットワークインフラストラクチャーは、各々トランシーバを含む物理的に離間されたベースステーション又はアクセスポイント（ＡＰ）を備えている。このような例示的システムでは、各ベースステーション又はＡＰは、通信システムの地理的エリア即ちセルを定義する。第１移動

ターミナルを使用して第２移動ターミナルと通信を行い、そして第１移動ターミナルがシステムのセル間を進行又は移動するときには、１つのベースステーションから別のベースステーションへのハンドオーバー通信により中断のない通信を行うことができる。このような通信ハンドオーバーは、ハンドオーバープロセスにより与えられる。

【０００４】

ＨＩＰＥＲＬＡＮ形式－２のような高性能の無線ローカルエリアネットワークは、３種類のハンドオーバーをサポートする。ＨＩＰＥＲＬＡＮ／２は、ポータブル装置とブロードバンドＩＰ、ＡＴＭ及びＵＭＴＳネットワークとの間に高速（通常２５Ｍｂ／ｓのデータレート）通信を与え、そして多数の媒体アプリケーションをサポートすることができ、典型的なアプリケーションは屋内である。ＨＩＰＥＲＬＡＮ／２は、ＩＰ、ＡＴＭ又はＵＭＴＳバックボーンに通常接続されたアクセスポイントと対話する移動及び固定ターミナルにより異なるインフラストラクチャーネットワーク（例えば、ＩＰ、ＡＴＭ及びＵＭＴＳ）へのローカルワイヤレスアクセスを与える。ネットワークにサービスするために多数のアクセスポイントが必要とされる。ワイヤレスネットワークは、全体として、移動性を与えるためにアクセスポイント間の接続のハンドオーバーをサポートする。典型的な動作環境は、ビジネスネットワーク及び家庭設備ネットワークを含む。ＨＩＰＥＲＬＡＮ／２アクセスネットワークの概要は、参考としてここに取り上げるヨーロピアン・テレコミュニケーションズ・スタンダーズ・インスティテュート（ＥＴＳＩ）ドキュメントＤＴＲ／ＢＲＡＮ－００２３０００２、１９９８年に掲載されている。

【０００５】

移動ターミナルのハンドオーバー判断に基づいて、セクターハンドオーバー（インターセクター）、無線ハンドオーバー（インターアクセスポイントトランシーバ／インターアクセスポイントハンドオーバー）、ネットワークハンドオーバー（インターアクセスポイント／インターネットワークハンドオーバー）、又は強制ハンドオーバーがＨＩＰＥＲＬＡＮ／２に従って生じる。

ハンドオーバーを実行する前に、移動ターミナルは、現在アクセスポイントに

より使用される周波数、及びハンドオーバーに対する候補であるアクセスポイントにより使用される周波数に関する当該測定値を収集しなければならない。サービング周波数の測定は、移動ターミナルが現在アクセスポイントに同期される間に移動ターミナルにより実行することができる。しかしながら、隣接するアクセスポイントの周波数を測定するためには、移動ターミナルが現在アクセスポイントから一時的に不存在にならねばならない。

【０００６】

移動ターミナル不存在手順の間に、移動ターミナルは、現在アクセスポイントから一時的に切断され、移動ターミナルは、隣接アクセスポイントに対する測定を行うことができる。この時間中には、移動ターミナルと現在アクセスポイントとの間で通信を行うことはできない。この不存在手順の一部分として、移動ターミナルは、それがｎフレームの間不存在になることを現在アクセスポイントに告げる。この不存在周期の間に、移動ターミナルは、現在アクセスポイントにより到達することができない。この不存在周期の後、現在アクセスポイントは、移動ターミナル活性化シーケンスをトリガーし、移動ターミナルを使用できるかどうかチェックする。

【０００７】

セクターハンドオーバー中には、アクセスポイントのアンテナセクターが変更され、同じアクセスポイントが全ハンドオーバーを制御する。セクターハンドオーバーが成功した後、移動ターミナルは、新たなセクターを経て通信する。無線ハンドオーバーは、アクセスポイント当たり２つ以上のトランシーバ、例えば、２つのアクセスポイントトランシーバと、１つのアクセスポイントコントローラとを有するアクセスポイントに関連している。無線ハンドオーバーは、移動ターミナルが、１つのアクセスポイントのカバレージエリアから、同じアクセスポイントによりサービスされる別のカバレージエリアへ移動するときに、実行される。無線ハンドオーバーは、データリンク制御（ＤＬＣ）層内で実行できるので、上位層プロトコル（ＨＬ）は含まれない。移動ターミナルが、別のアクセスポイントコントローラへのハンドオーバーの必要性を検出したとき、移動ターミナルは、現在アクセスポイントに依然同期することができる。この場合に、移動ター

ミナルは、それが別のアクセスポイントコントローラへのハンドオーバーを遂行することをそのアクセスポイントコントローラに通知する。無線ハンドオーバーの場合は、進行中の接続、セキュリティパラメータ等に関する全ての当該情報がアクセスポイントに得られ、従って、この情報は再ネゴシエーションされない。

【０００８】

ネットワークハンドオーバーは、移動ターミナルが１つのアクセスポイントから別のアクセスポイントへ移動するときに実行される。移動ターミナルは、無線制御リンク（ＲＬＣ）インスタンスのサービスエリアを立ち去るので、ネットワークハンドオーバーは、収斂層（ＣＬ）及びＨＬ（必要に応じて）並びにＤＬＣＩを含む。ＨＬ関連性及び接続を維持するために、バックボーンを通る特定のシグナリングが必要となる。移動ターミナルは、別の（ターゲット）アクセスポイントへのハンドオーバーの必要性を検出すると、現在アクセスポイントに依然同期されてもよい。この場合に、移動ターミナルは、それが別のアクセスポイントへのハンドオーバーを実行することを現在アクセスポイントに通知する。通知されたアクセスポイントは、次いで、その移動ターミナルへの通信を停止するが、指示があったときには特定の時間中その関連性を維持しなければならない。

【０００９】

強制ハンドオーバーは、現在アクセスポイントのセルを立ち去るようある移動ターミナルに命令する機会を現在アクセスポイントに与える。強制ハンドオーバーは、アクセスポイントがＦｏｒｃｅ＿Ｈａｎｄｏｖｅｒ信号を移動ターミナルに送信することにより開始される。１つの手順において、移動ターミナルは、新たなセルを見つけるかどうかに関わりなく、通常のハンドオーバーを実行してその古いセルを立ち去る。第２の手順では、移動ターミナルは、ハンドオーバーが失敗した場合に古いアクセスポイントに戻る機会を有する。

ＨＩＰＥＲＬＡＮ／２特徴のこれ以上の説明については、参考としてここに取り上げるＥＴＳＩ規格化団体により提供された「ブロードバンド無線アクセスネットワーク（ＢＲＡＮ）：ＨＩＰＥＲＬＡＮ形式２機能的仕様：無線リンク制御（ＲＬＣ）」を参照されたい。

【００１０】

限定された地理的エリア、例えば、ビルやビル内のオフィス仕事場により包囲された限定されたエリアを包囲するために、多数の形式のワイヤレス通信システムが実施されそして他のものが提案されている。マイクロセルラーネットワーク、プライベートネットワーク及びＷＬＡＮのようなワイヤレス通信システムは、このようなシステムの一例である。

ワイヤレス通信システムは、通常、取締り又は準取締り団体により施行された規格に準拠して構成される。例えば、ＩＥＥＥ（インスティテュート・オブ・エレクトリカル・アンド・エレクトロニック・エンジニアリング）により施行されたＩＥＥＥ８０２．１１規格は、一般に商業用２．４ＧＨｚワイヤレスＬＡＮに関するワイヤレスローカルエリアネットワーク（ＬＡＮ）規格である。この８０２．１１規格は、ワイヤレスターミナルとベースステーションとの間及びワイヤレスターミナル間のインターフェイスを規定する。物理層及び媒体アクセス制御（ＭＡＣ）層に関する標準は、このような規格に規定されている。この規格は、互換性のある物理層を含む種々の装置間に自動的に媒体を振り分けできるようにする。この規格においては、一般に、ＭＡＣ層により、衝突回避（ＣＳＭＡ／ＣＡ）通信スキムを伴う搬送波感知多重アクセスを使用して、非同期データ転送が行われる。

【００１１】

ＩＥＥＥ８０２．１１規格は、このような規格に準じて相互に動作できるように構成された移動ターミナルを使用することによりワイヤレス通信を行うためのものであるが、リアルタイムワイヤレスサービスについては充分に規定していない。例えば、この規格を実施する場合に、あるＡＰから別のＡＰへの通信ハンドオーバー中に著しいクオリティロスに時々遭遇する。相当数のデータフレームが失われるか又は遅延され、その結果、通信クオリティが失われるか、又は通信が終了することすらある。それ故、特にリアルタイムワイヤレスサービスについては、ＩＥＥＥ８０２．１１規格に規定された以外の動作モードが必要とされる。既存のＩＥＥＥ８０２．１１規格に準じた動作に比して通信クオリティの改善を許す所有権付き機能が提案されている。このような所有権付き機能を実行するように動作できるＡＰ及び移動ターミナルは、所有権モード可能と称される。

【００１２】

しかしながら、移動ターミナルと、移動ターミナルが通信するときに通るＡＰとで構成された通信対の両端は、所有権モードでの動作が可能でなければならない。通信対の両端が所有権モードに準じて一緒に動作できない場合には、ＩＥＥＥ８０２．１１規格に準じた従来の動作が必要とされる。それ故、通信対の両端が所有権モードで動作するのを許す前に、通信対の両端が所有権モードに準じて動作できる能力について決定しなければならない。

上記の特許出願は、通信対の両端が所有権モードで一緒に動作できるかどうか識別するよう動作できる装置を提供する。この装置は、対の互換性が存在すると決定されたときに所有権モードで動作するように通信対の両端をアクチベートし、そしてその後、移動ターミナルが、第１ＡＰによりサービスされるセルから、第２ＡＰによりサービスされるセルへ物理的に移動したとすれば、ハンドオーバー手順の間に所有権モード動作を維持するように動作する。

【００１３】

この特許出願の装置により与えられる貴重な特徴に加えて、このようなＡＰ－ＡＰハンドオーバーが発生するときにセキュリティ関連性を再確立することが望ましい。

多くの顧客、特に、ビジネス環境は、高度なデータセキュリティを必要としており、このデータセキュリティは、ＷＬＡＮインストールを使用することにより妥協することができない。ＷＬＡＮへのアクセスは、物理的に制限することができないので、送信されたデータ及びネットワーク要素を保護するために、暗号化方法を使用することが習慣となっている。現在のＩＥＥＥ８０２．１１及びＩＴＥＦインターネット規格は、ワイヤレスリンクを経ての機密データ通信即ちインターネットプロトコルセキュリティ（ＩＰＳＥＣ）を与えるための２つの相補的なメカニズムを与える。このＩＰＳＥＣは、２つのＩＰホスト間にＦＯＲ機密通信を与えるＩＰベースのセキュリティプロトコルである。ＩＰＳＥＣプロトコルは、バーチャルプライベートネットワーク（ＶＰＮ）を構築する際に一般に使用される。

【００１４】

ＷＬＡＮシステムでは、ＩＰｓｅｃプロトコルを使用して、データパケットに対する端－端セキュリティを与えることができ、このセキュリティは、送信されるデータパケットを認証及び／又は暗号化することにより与えられる。ＩＰｓｅｃは、対称的な暗号化を使用し、これは通信リンクの両端に同じ暗号及び／又は認証キーを使用する必要がある。ＩＫＥのようなシール可能なキーマネージメントプロトコルを使用して、ＩＰｓｅｃスタックに対する対象的キーを発生することができる。

インターネットキー交換（ＩＫＥ）のキーマネージメントプロトコルは、初期の移動ターミナル／アクセスポイント間連中にＩＰレベルセキュリティ関連性を確立するのに有用であるが、通信ハンドオーバーの必要が生じたときには、ＩＫＥ又は他の同様のプロトコルの使用がハンドオーバーの実行に著しい時間遅延を与える。というのは、このようなプロトコルは、多数のメッセージの交換を必要とし、パブリック暗号キーの使用が多大な計算を必要とするからである。ペイロードトラフィックのハンドオーバーは、新たなＡＰと移動ターミナルとの間にアクティブなセキュリティ関連性が確立された後でなければ再開できないので、ＩＫＥキー管理プロトコル又は他のこのようなプロトコルを使用すると、ハンドオーバー中に問題が生じる。

【００１５】

動的な暗号キー即ちセッション依存の動的なキーを伴うセキュリティプロトコルが移動ターミナルとＡＰとの間に適用されたときには、移動ターミナルが、ワイヤレス無線ネットワーク又はシステムにより形成されるカバレージ内を移動するときに、あるＡＰから別のＡＰへアクティブなセキュリティ関連性を転送するためのメカニズムを見出すことが望ましい。

このような背景情報に鑑み、本発明は、ＷＬＡＮ通信ハンドオーバー中にキーを管理しそしてセキュリティ関連性を再確立するための低又は短遅延の方法／装置であって、ハンドオーバー中に端－端セキュリティ関連性（例えば、移動ターミナルとサーバーとの間のＩＰｓｅｃペイロード接続）を変更する必要がなく、そしてハンドオーバーが移動ターミナルと新たな及び古いＡＰとの間のセキュリティ機能にしか影響しないような方法／装置を提供する。

【００１６】

【発明の開示】

本発明は、無線通信、ＩＥＥＥ８０２．１１　２．４ＧＨｚＷＬＡＮ規格、高性能無線ローカルエリアネットワーク（ＨＩＰＥＲＬＡＮ）、ＥＴＳＩ　ＨＩＰＥＲＬＡＮ形式２規格、及びワイヤレスターミナルとネットワーク要素との間のＩＰＳＥＣレベルセキュリティ関連性に係る。本発明は、ＥＴＳＩ　ＢＲＡＮやＩＥＥＥ８０２．１１を一例として含むいかなるＩＰベースのワイヤレスネットワークにも使用することができる。更に、本発明は、移動ターミナルが２つのＩＰＳＥＣルーターエンティティ間を移動するときに、ワイヤレスターミナルが、ワイヤレスアクセスポイントでないエンドポイントと通信する場合に使用することができる。

【００１７】

本発明は、ＩＥＥＥ８０２．１１又はＨＩＰＥＲＬＡＮのような無線通信システムにハンドオーバー事象が発生するときに既存のセキュリティ関連性を再確立するための効率的な方法／装置を提供する。本発明の動作は、ハンドオーバーの性能を高め、そして新たなＡＰと移動ターミナルとの間のセキュリティ関連性を再ネゴシエーションするのに関連した遅延を最小にする。

本発明は、ネットワーク内にハンドオーバーが発生するときに移動ターミナルとワイヤレス通信ネットワークとの間に確立されたセキュリティ関連性を維持する効率的な方法を提供する。本発明を利用する一例は、ＷＬＡＮ内の移動ターミナルとＡＰとの間にインターネットプロトコルセキュリティ（ＩＰｓｅｃ）ベースのセキュリティ関連性を有するＷＬＡＮである。しかしながら、本発明は、ＨＩＰＥＲＬＡＮ／２無線レベルセキュリティ機能のようないかなる形式の動的セキュリティ関連性を維持するのにも使用できる。

【００１８】

本発明によれば、ハンドオーバー事象中の移動ターミナルの認証は、チャレンジ／応答手順により達成される。このチャレンジ／応答手順によれば、新たなＡＰが移動ターミナルにチャレンジを送信し、移動ターミナル（ＭＴ）は、それに応答して、新たなＡＰに応答を送信する。

移動ターミナルとＡＰとで作られる通信対の両端に対する認証キーは、最初に、スケーリング可能なキーマネージメントプロトコル、例えば、インターネットキー交換（ＩＫＥ）により発生される。各ハンドオーバー中に新たな及び異なるキーの交換の必要性を回避するために、ワイヤレス通信システム内にある種々のＡＰ間でセキュリティ関連性が転送される。

【００１９】

キー及びそれに関連した情報は、ハンドオーバープロセス中に新たなＡＰにより要求され、そしてキー及び他の情報は、古いＡＰと新たなＡＰとの間を通過する１つ以上のハンドオーバーメッセージにおいて古いＡＰから新たなＡＰへ転送される。認証チャレンジの交換及びそれに対する応答は、新たなＡＰと、ハンドオーバーに含まれる移動ターミナルとの間に生じるハンドオーバーシグナリングに一体化される。

本発明の特徴によれば、メッセージは、媒体アクセス制御（ＭＡＣ）メッセージである。

アクセスポイント認証を与える本発明の特徴は、望ましいものであるが、任意の特徴であることに注意されたい。

アクセスポイント間では機密の接続が好ましいが、このような特徴は、本発明の精神及び範囲によって要求されるものではない。

【００２０】

【発明を実施するための最良の形態】

本発明のこれら及び他の特徴並びに効果は、添付図面を参照した以下の説明により当業者に明らかとなろう。

図１は、移動ターミナル１２が一例である複数の移動ターミナル間で及びそれらと無線通信するための通信システムを例示する図である。別の例では、アクセスポイントが無線インターフェイス及び固定ネットワークブリッジをカバーし、アクセスポイントが固定ネットワークに接続され、この例は、図１に示すＣＣＵを必要としない。通信システム１０は、ＩＥＥＥ８０２．１１規格に規定されたように、そしておそらくは上記特許出願に開示された所有権付きの動作モードに準拠するように、複数の移動ターミナル１２との無線通信を与えるＷＬＡＮを形

成する。他の通信システムも同様であり、本発明の動作は、このような他の通信システムでも作用し得る。

【００２１】

ＷＬＡＮ１０は、２つの離間された地理的位置に個々に配置された複数の離間されたＡＰ１４及び１１４を含む。２つのＡＰ１４，１１４しか示されていないが、実際には、非常に多数のＡＰが使用される。ＡＰ１４、１１４は、ベースステーション又はリモートアンテナ装置（ＲＡＤ）とも称される。「アクセスポイント」、「ＡＰ」又は「ａｐ」という語は、ここでは、通信システム１０のネットワークインフラストラクチャーにアクセスするポイントを形成する装置を示すために一般的に使用される。「移動ターミナル」、「ＭＴ」又は「ｍｔ」という語は、アクセスポイントにアクセスするポイント形成する装置を示すために一般的に使用される。

【００２２】

ＡＰ１４、１１４の各々は、移動ターミナルが特定のＡＰの通信範囲内に位置するときに移動ターミナル１２と無線通信信号をやり取りすることのできる無線トランシーバ回路１６を備えている。一般に、移動ターミナル１２は、所定のアクセスポイントの近くにあって且つそれにより定義された地理的エリア即ちセル１８、１１８内に位置するときに、ＡＰ１４、１１４と通信する。図１において、セル１８はアクセスポイント１４に関連され、移動ターミナル１２はセル１８内にあり、そしてセル１１８は、アクセスポイント１１４に関連している。モードセレクタ３４は、本発明が所有権付き無線リンクレベルメッセージを使用して実施されるときだけ含まれ、これは、本発明に必須の実施ではない。

【００２３】

アクセスポイント１４、１１４は、中央制御ユニット（ＣＣＵ）２２に接続される。このＣＣＵ２２は、通常、ハブ又はＩＰルーターである。ＣＣＵ２２は、外部通信ネットワークバックボーン２４への接続を与える。図示されていないが、通常、他の通信ステーション及び他の通信ネットワークのような他の通信装置が通信ネットワークバックボーン２４に接続される。このように、移動ターミナル１２と、通信ネットワークバックボーン２４に直接的又は間接的に接続された

通信ステーションとの間に通信を与えるように、通信経路を形成することができる。又、複数の移動ターミナル１２間のローカル通信も許される。移動ターミナル１２の対間の通信においては、それらの間に形成される通信経路が２つの個別の無線リンクを含む。

【００２４】

ＡＰ１４、１１４は、各ＡＰの動作に関連した種々の制御機能を実行する制御要素２８を備えている。図１において、制御要素２８は、各々、比較器３２、モードセレクタ３４及びハンドオーバー利用性決定装置３６を含むように示されており、これらの制御要素は、機能的なもので、例えば、処理回路により実行できるアルゴリズムのような所望のやり方で実施される。別の実施形態では、このような要素により実行される機能は、どこかに配置され、例えば、ブロック２８’で示すように移動ターミナル１２に配置されるか、又はブロック２８”で示すようにＣＣＵ２２に配置される。従って、制御要素により実行される機能は、多数の異なる装置間に分散することができる。

本発明によれば、比較器３２は、セキュリティ機能を含み、そしてブロック２８は、媒体アクセス制御（ＭＡＣ）機能を含むことに注意されたい。

【００２５】

図１の構造及び構成において、上述した特許出願に教示されたように、ＡＰ１４、１１４と移動ターミナル１２とで形成された通信対は、その通信対が両方とも所有権モードに適合しないと決定されたときにはＩＥＥＥ８０２．１１標準モードに準じて動作でき、或いはその通信対の両メンバーが所有権モード可能であると決定されたときには所有権モードに準じて動作できる。この結果を生じさせるために、比較器３２は、通信対を形成する移動ターミナル及びアクセスポイントの両方の動作し得るモードを識別する識別子を受信する。次いで、モードセレクタ３４は、移動ターミナルとアクセスポイントとの間の通信のために標準的な動作モード又は所有権動作モードを選択する。

【００２６】

移動ターミナル１２の物理的な位置が所与の通信セッション中にセル１８からセル１１８へ変化するときには、移動ターミナル１２は、ＡＰ１４によりサービ

スされる第１地理的エリア１８を出て、ＡＰ１１４によってサービスされる第２地理的エリア１１８に入る。このセル対セル又はエリア対エリア移動は、第１エリア１８に関連した古いＡＰ１４から、第２エリア１１８に関連した新たなＡＰ１１４への通信のハンドオーバーを必要とし、これにより、移動ターミナル１２との連続した通信が許される。

ハンドオーバー利用性決定装置３６は、通信ハンドオーバーが可能である利用可能なＡＰの指示を移動ターミナル１２に与え、この利用性は、通信ハンドオーバーに利用できるＡＰの認識を含む利用可能なアクセスポイントのリスト３８に含まれる。

【００２７】

利用可能なアクセスポイントのリスト３８は、選択された時間間隔で移動ターミナル１２に通信することもできるし、又はアクセスポイントのリスト３８は、移動ターミナルが最初にアクチベートされるときに各移動ターミナル１２に与えることもできるし、或いはネットワークプレフィックス又はネットワークプレフィックスのリストを使用して同じ目的を達成することもできる。

本発明のこの説明では、移動ターミナル１２と、現在の又は古いＡＰ１４との間にセキュリティ関連性（ＳＡ）が存在すると仮定する。即ち、移動ターミナル１２及びＡＰ１４は、同じ共通セットのキーと、セキュリティ機能を達成するのに必要な他の情報とを共有すると仮定する。本発明によれば、この確立されそして共有されるセキュリティ関連性が、移動ターミナルがセル１８からセル１１８へ移動するときに機密形態で古いＡＰ１４から新たなＡＰ１１４へ転送される。この転送は、転送を行うに必要なメッセージの数を最小にし、そしてパブリックキー暗号の使用を排除することにより、非常に迅速に行われる。その結果、移動ターミナル１２への及びそこからのペイロードトラフィックの中断が最小にされ、この種の中断は、ボイス・オーバーＩＰ（ＶＯＩＰ）及び映像配信のようなリアルタイムサービスにとって非常に重大である。

【００２８】

本発明によれば、通信リンク（即ち移動ターミナル１２及びＡＰ１４を伴うリンク）の両端に対する認証キー又はセキュリティ関連性は、ＩＫＥのようなシー

ル可能なキーマネージメントプロトコルによって発生され、ディフィー・ヘルマンのキー交換プロトコルも使用できることに注意されたい。

その後、移動ターミナル１２がセル１８及びそのＡＰ１４からセル１１８及びそのＡＰ１１４へ移動するときに、ハンドオーバープロセス中の認証が本発明の簡単なチャレンジ／応答手順によって達成される。又、セキュリティ関連性は、古いＡＰ１４と新たなＡＰ１１４との間に転送され、従って、古いＡＰ１４から新たなＡＰ１１４へのハンドオーバー中に新たなキー交換を行う必要性が排除される。

【００２９】

チャレンジ／応答手順の間に、新たなＡＰ１１８は、移動ターミナル１２へチャレンジを送信し、その際に、移動ターミナル１２は、新たなＡＰ１１８に応答を送信する。更に、移動ターミナル１２は、新たなＡＰ１１８をハンドオーバー中に同様に認証する。

キー及びそれに関連した情報が新たなＡＰ１１４により要求され、その際に、それらは古いＡＰ１４から新たなＡＰ１１４へハンドオーバーメッセージにおいて転送される。同様に、認証チャレンジの交換及びそれに対する応答は、新たなＡＰ１１４と、移動ターミナル１２との間に生じるハンドオーバーシグナリングに一体化される。

【００３０】

図２は、本発明による順方向ハンドオーバー（ＨＯ）プロセス２０を示し、これは、本発明の好ましい実施形態である。順方向ハンドオーバープロセス２０では、移動ターミナル（ＭＴ又はｍｔ）と新たなアクセスポイント（ＡＰ又はａｐ）１１４との間にハンドオーバーシグナリングが送信される。この形式のハンドオーバーは、特に、無線リンク２１が事前の警告なしに失われるときに特に有用である。

図３は、本発明による逆方向ハンドオーバー（ＨＯ）プロセス３０を示す。逆方向ハンドオーバープロセス３０においては、古いＡＰ１４と通信する移動ターミナル１２によってハンドオーバーが要求され、その結果、図２に示したものとは若干異なるメッセージシーケンスが生じる。逆方向ハンドオーバー中の有益な

オプションは、古いＡＰ１４から移動ターミナル１２へ認証チャレンジを搬送する無線インターフェイスメッセージ３１を使用して、逆方向ハンドオーバー３３もトリガーすることである。即ち、古いＡＰ１４から切断しそしてセキュリティ関連性（ＳＡ）３５が移動ターミナル１２に対して既に準備された新たなＡＰ１４へ接続すべきであることを移動ターミナル１２に指示するために、認証チャレンジ３１が使用される。

【００３１】

ここで使用される「古いＡＰ」という語は、移動ターミナル１２が最初に又は現在通信しているアクセスポイント１４のようなアクセスポイントを意味する。従って、「古いＡＰ」という語は、通信ハンドオーバーが必要とされる時点で移動ターミナル１２が通信している「現在ＡＰ」も意味する。

ここで使用する「新たなＡＰ」という語は、移動ターミナル１２が古いセル１８から新たなセル１１８へ地理的に移動したために移動ターミナル１２が通信を開始しなければならないアクセスポイント１１４のようなアクセスポイントを意味する。従って、「新たなＡＰ」という語は、通信ハンドオーバーが完了した後に移動ターミナル１２が通信する「将来のＡＰ」も意味する。

【００３２】

図２及び３には、ＩＥＥＥ８０２．１１メッセージ名が使用され、そしてハンドオーバーメッセージの付加的なパラメータが示されている。しかしながら、このメッセージ名は、本発明の範囲にとって重要ではない。というのは、本発明は、ＩＥＥＥ８０２．１１以外のシステムでも実施できるからである。しかしながら、図２及び３の拡張ＭＡＣ（媒体アクセス制御）メッセージを使用して、無線インターフェイスを経て付加的なパラメータを搬送することは、付加的なメッセージを送信する必要性が排除されるという点で有益である。

セキュリティを保証するためには、キーを搬送するメッセージを暗号化するのが望ましい。それ故、ＡＰ１４、１１４間でのセキュリティ関連性即ちＳＡ及び他の制御トラフィックの転送は、ＩＰｓｅｃにより暗号化されそして認証されるものとして示されている。

【００３３】

従って、ハンドオーバーが必要とされるように移動ターミナル１２がセル１８、１１８に対して物理的に移動されたことを決定する特定の手段は、本発明にとって重要ではない。例えば、その手順は、移動支援ハンドオーバー手順を使用する従来の時分割セルラーシステムに使用されるものと同様でよい。一般に、移動ターミナル１２は、セル１８、１１８のような隣接セルのベースステーション又はＡＰの制御チャンネルに、例えば、タイミングを合わせた間隔で同調する。次いで、これらの制御チャンネルにブロードキャストされる信号の信号強度、又はビットエラー率のような他の信号特性が移動ターミナル１２により測定され又は感知される。移動ターミナル１２におけるこの測定をベースとするアップリンク信号は、次いで、移動ターミナルによりネットワーク１０へ送信され、その際に、ネットワーク１０は、通信ハンドオーバーを行うべきかどうか決定する。ハンドオーバーが必要であると決定された場合には、命令が移動ターミナル１２に送信され、そして図２又は３の通信ハンドオーバープロセスが開始される。

【００３４】

図４Ａないし４Ｃは、移動ターミナル１２がセル１８からセル１１８へ移動するときに移動ターミナル１２の通信ハンドオーバーが古いＡＰ１４及び新たなＡＰ１１４に対して行われる順方向ハンドオーバープロセス２０を示す別の図である。この図において、移動ターミナル即ちＭＴは、「ｍｔ」とも称され、そしてアクセスポイント即ちＡＰは、「ａｐ」とも称される。

図４Ａを参照すれば、順方向ハンドオーバープロセス２０は、ハンドオーバーが要求されることを指示する事象４０１のイエス出力４００により移動ターミナル１２において開始される。移動ターミナル１２は、ここで、ファンクション４０２において、無線ハンドオーバー機能をアクチベートするように動作する。

ファンクション４０３において、移動ターミナル１２は、新たなＡＰ１１４へチャレンジを発生し、その際に、ファンクション４０４において、「ｍｔ＿ｃｈａｌｌｅｎｇｅ」を含むＭＡＣ＿ＲＥＡＳＳＯＣＩＡＴＥ＿ＲＥＱメッセージが新たなＡＰ１１４へ送信される。

【００３５】

ファンクション４０５において、新たなＡＰ１１４は、メッセージ４０４を受

け入れ、その際に、新たなＡＰ１１４は、ファンクション４０６において、ハンドオーバー要求を古いＡＰ１４へ送信するように動作する。

古いＡＰ１４は、ここで、ファンクション４０７において、セキュリティ関連性パラメータＳＡ、ＳＡをそのセキュリティ関連性データベースから検索するように動作する。次いで、古いＡＰ１４は、ファンクション４０８において、パラメータＳＡ、ＳＡを含むハンドオーバー要求を新たなＡＰ１１４へ送信するように動作する。

図４Ｂを参照すれば、新たなＡＰ１１４は、ここで、ファンクション４０９においてセキュリティ関連性（ＳＡ）を形成するように動作し、ファンクション４１０において移動ターミナル１２を認証するためのチャレンジを発生するように動作し、ファンクション４１１において、図４Ａのメッセージ４０４に含まれた「ｍｔ＿ｃｈａｌｌｅｎｇｅ」に対する応答を計算するように動作し、そしてファンクション４１２において、ＭＡＣ＿ＡＵＴＨＥＮＴＩＣＡＴＥ＿ＲＥＱメッセージを移動ターミナル１２へ送信するように動作する。メッセージ４１２は、ファンクション４１１の動作により計算された「ａｐ＿ｒｅｓｐｏｎｓｅ」を含み、ファンクション４１０の動作により発生された「ａｐ＿ｃｈａｌｌｅｎｇｅ」を含み、そして「他の情報」を含む。

【００３６】

移動ターミナル１２は、ここで、ファンクション４１３においてそのセキュリティ関連性パラメータを更新するように動作し、ファンクション４１４においてメッセージ４１２により受け取られた「ａｐ＿ｃｈａｌｌｅｎｇｅ」に対する応答を計算するように動作し、そしてファンクション４１５において、メッセージ４１２により受け取られた「ａｐ＿ｒｅｓｐｏｎｓｅ」を正しい又は予想される応答と比較するように動作する。

ファンクション４１５により実行された比較が正しい比較を生じた場合には、ファンクション４１６は、新たなＡＰ１１４を認証するように動作し、その際に、ファンクション４１７は、ＭＡＣ＿ＡＵＴＨＥＮＴＩＣＡＴＥ＿ＲＥＳＰメッセージを新たなＡＰ１１４へ送信するように動作し、このメッセージは、ファンクション４１４で計算された「ｍｔ＿ｒｅｓｐｏｎｓｅ」を含む。

【００３７】

図４Ｃを参照すれば、ファンクション４１８において、新たなＡＰ１１４は、メッセージ４１７により受け取られた「ｍｔ＿ｒｅｓｐｏｎｓｅ」を適切な又は正しい応答と比較するように動作し、そしてこの比較が正しい比較を生じるときには、ファンクション４１９が移動ターミナル１２を認証するように動作する。新たなＡＰ１１４は、次いで、ファンクション４２０において、ＭＡＣ＿ＲＥＡＳＳＯＣＩＡＴＥ＿ＲＥＳＰメッセージを移動ターミナル１２へ送信するように動作し、その際に、ハンドオーバーが完了し、そしてその後、移動ターミナル１２は、ファンクション４２１において、新たなＡＰ１１４を使用してそのペイロードトラフィックを再開するように動作する。

図５Ａないし５Ｃは、通信ハンドオーバーが移動ターミナル１２について古いＡＰ１４及び新たなＡＰ１１４に対して行われる逆方向ハンドオーバープロセス３０を示す別の図である。この図では、移動ターミナル即ちＭＴが「ｍｔ」とも称され、そしてアクセスポイント即ちＡＰが「ａｐ」とも称される。

【００３８】

図５Ａを参照すれば、ハンドオーバーが要求されたことを指示する事象５０１のイエス出力５００により逆方向ハンドオーバープロセス３０が移動ターミナル１２において開始される。移動ターミナル１２は、ここで、ファンクション５０２においてハンドオーバー要求を古いＡＰ１４へ送信するように動作する。

メッセージ５０２が古いＡＰ１４に受け取られると、ファンクション５０３はそのメッセージを受け入れ、ファンクション５０４は、セキュリティ関連性パラメータＳＡ、ＳＡをそのセキュリティ関連性（ＳＡ）データベースから検索するように動作し、そしてファンクション５０５は、パラメータＳＡ、ＳＡを含むハンドオーバー要求を新たなＡＰ１１４へ送信するように動作する。

【００３９】

メッセージ５０５で受け取られたパラメータＳＡ、ＳＡを使用して、新たなＡＰ１１４は、ここで、ファンクション５０６において、それ自身のセキュリティ関連性（ＳＡ）を生成するように動作する。新たなＡＰ１１４は、次いで、ファンクション５０７において、移動ターミナル１２を認証するためのチャレンジを

発生するように動作し、そしてファンクション５０８において、ハンドオーバー要求が古いＡＰ１４へ送信され、この要求５０８は、ファンクション５０７で発生された「ａｐ＿ｃｈａｌｌｅｎｇｅ」及び「他の情報」を含む。

図５Ｂを参照すれば、メッセージ５０８に応答して、古いＡＰ１４は、ファンクション５０９において、ＭＡＣ＿ＤＩＳＡＳＳＯＣＩＡＴＥメッセージを移動ターミナル１２へ送信するように動作し、このメッセージは、古いＡＰ１４がメッセージ５０８により新たなＡＰ１１４から受信した「ａｐ＿ｃｈａｌｌｅｎｇｅ」及び「他の情報」を含んでいる。

【００４０】

メッセージ５０９に応答して、移動ターミナル１２は、その無線ハンドオーバーファンクションを５１０においてアクチベートする。ファンクション５１１において、移動ターミナル１２は、ここで、そのセキュリティ関連性パラメータを更新し、ファンクション５１２において、移動ターミナル１２は、メッセージ５０８及び５０９の「ａｐ＿ｃｈａｌｌｅｎｇｅ」に対する応答を計算するように動作し、ファンクション５１３において、移動ターミナル１２は、新たなＡＰ１１４を認証するためのチャレンジを発生するように動作し、そしてファンクション５１４において、移動ターミナル１２は、ＭＡＣ＿ＲＥＡＳＳＯＣＩＡＴＥ＿ＲＥＱメッセージを新たなＡＰ１１４へ送信するように動作する。メッセージ５１４は、ファンクション５１１で計算された「ｍｔ＿ｒｅｓｐｏｎｓｅ」、ファンクション５１２で発生された「ｍｔ＿ｃｈａｌｌｅｎｇｅ」及び「他の情報」を含む。

【００４１】

図５Ｃを参照すれば、ファンクション５１５は、移動ターミナル１２の認証を与え、ファンクション５１６は、メッセージ５１３により受け取られた「ｍｔ＿ｒｅｓｐｏｎｓｅ」を正しい又は予想応答と比較し、ファンクション５１７は、メッセージ５１３により受け取られた「ｍｔ＿ｃｈａｌｌｅｎｇｅ」に対する応答を計算し、そしてファンクション５１８は、ＭＡＣ＿ＲＥＡＳＳＯＣＩＡＴＥ＿ＲＥＳＰ＿ＥＮＨメッセージを移動ターミナル１２に送信するように動作し、メッセージ５１８は、ファンクション５１７により計算された「ａｐ＿ｒｅｓｐ

ｏｎｓｅ」を含んでいる。

ファンクション５１９において、移動ターミナル１２は、新たなＡＰ１１４を認証するように動作し、これは、ファンクション５２０において、メッセージ５１８に含まれた「ａｐ＿ｒｅｓｐｏｎｓｅ」を正しい又は予想応答と比較することで行われ、その正しい比較の結果として、ファンクション５２１は、移動ターミナル１２が新たなＡＰ１１４を使用してペイロードトラフィックを再開するようにさせる。

【００４２】

以上のことから明らかなように、本発明は、所定の移動ターミナル１２との通信が第１アクセスポイント１４から第２アクセスポイント１１４へハンドオーバーされるときに情報のセキュリティを与える方法及び装置を提供する。複数のアクセスポイントを有する通信システム１０が設けられ、各アクセスポイントは、通信システム１０によりサービスされる全地理的エリア内の異なる地理的エリアにサービスし、そして複数の移動ターミナル１２が設けられ、これら移動ターミナルは、全地理的エリア内及び異なる地理的エリア間を個々に物理的に移動することができる。

本発明のハンドオーバープロセス／装置において、最初に、所与の移動ターミナル１２が、第１アクセスポイント１４との通信作用から、第２アクセスポイント１１４との通信作用へと移動するときに、それが感知される（図４Ａの４０１及び図５Ａの５０１を参照）。

【００４３】

このような移動が感知されると、セキュリティ関連性パラメータが第１アクセスポイント１４からフェッチされ（図４Ａの４０７及び図５Ａの５０４を参照）、その検索されたセキュリティ関連性パラメータに基づき第２のアクセスポイント１１４においてセキュリティ関連性が生成され（図４Ｂの４０９及び図５Ａの５０６を参照）、そしてその検索されたセキュリティ関連性パラメータに基づき所与の移動ターミナル１２においてセキュリティ関連性が生成される（図４Ｂの４１３及び図５Ｂの５１０を参照）。

又、このような移動が感知されると、所与の移動ターミナル１２から第２のア

クセスポイント１１４へ認証アクセスポイントチャレンジが送信され（図４Ａの４０４及び図５Ｂの５１３を参照）、そして第２のアクセスポイント１１４から所与の移動ターミナル１２へ認証移動ターミナルチャレンジが送信される（図４Ｂの４１２及び図５Ａの５０８を参照）。上記アクセスポイントチャレンジは、本発明の任意の特徴であることに注意されたい。

【００４４】

所与の移動ターミナル１２から受け取られた認証アクセスポイントチャレンジに応答して、第２アクセスポイント１１４は、ここで、認証アクセスポイント応答を発生し（図４Ｂの４１１及び図５Ｃの５１６を参照）、そしてこの認証アクセスポイント応答は、所与の移動ターミナル１２へ送信される（図４Ｂの４１２及び図５Ｃの５１７を参照）。

第２アクセスポイント１１４から受け取られた認証移動ターミナルチャレンジに応答して、所与の移動ターミナル１２は、ここで、認証移動ターミナル応答を計算し（図４Ｂの４１４及び図５Ｂの５１１を参照）、そしてこの認証移動ターミナル応答は、第２アクセスポイント１１４へ送信される（図４Ｂの４１７及び図５Ｂの５１３を参照）。

【００４５】

所与の移動ターミナル１２における第１比較は、ここで、第２アクセスポイント１１４から受け取られた認証アクセスポイント応答を、正しい又は予想応答と比較するように動作し（図４Ｂの４１５及び図５Ｃの５１９を参照）、そして第２アクセスポイント１１４における第２比較は、ここで、所与の移動ターミナル１２から受け取った認証移動ターミナル応答を、正しいまたは予想応答と比較するように動作する（図４Ｃの４１８及び図５Ｃの５１５を参照）。

最終的に、第１比較及び第２比較の結果に基づいて所与の移動ターミナル１２と第２アクセスポイント１１４との間で通信が開始される（図４Ｃの４２１及び図５Ｃの５２０を参照）。

【００４６】

図６及び７は、本発明の２つの付加的な実施形態を示す。図６及び７の実施形態は、その特定の細部が相違するが、図６及び７の実施形態の内容は、本発明の

上記図２、３、４Ａ－４Ｂ及び５Ａ－５Ｂと比較することにより容易に明らかとなろう。

以上、本発明の好ましい実施形態を詳細に説明したが、これは、本発明の精神及び範囲を何ら限定するものではなく、当業者であれば、特許請求の範囲に規定された本発明の範囲内で他の実施形態が容易に明らかとなろう。

【図面の簡単な説明】

【図１】

本発明の実施形態が作用する通信システムを示す図である。

【図２】

本発明による順方向ハンドオーバープロセスを示す図である。

【図３】

本発明による逆方向ハンドオーバープロセスを示す図である。

【図４Ａ】

図２の順方向ハンドオーバープロセスを示す別の図である。

【図４Ｂ】

図２の順方向ハンドオーバープロセスを示す別の図である。

【図４Ｃ】

図２の順方向ハンドオーバープロセスを示す別の図である。

【図５Ａ】

図３の逆方向ハンドオーバープロセスを示す別の図である。

【図５Ｂ】

図３の逆方向ハンドオーバープロセスを示す別の図である。

【図５Ｃ】

図３の逆方向ハンドオーバープロセスを示す別の図である。

【図６】

本発明によるＨＩＰＥＲＬＡＮ／２強制ハンドオーバーを示す図である。

【図７】

本発明によるＨＩＰＥＲＬＡＮ／２順方向ハンドオーバーを示す図である。

【図１】

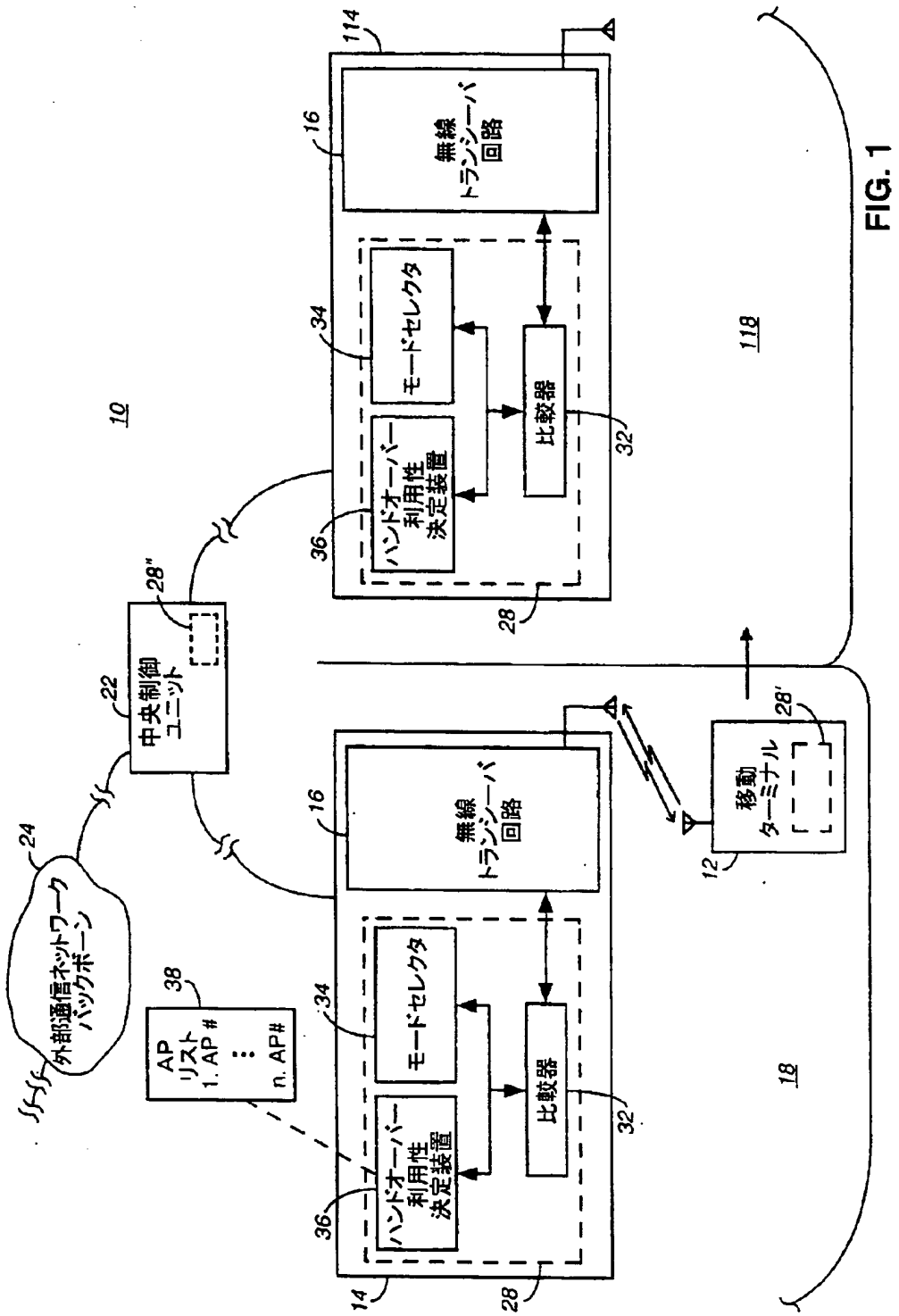

10
114
16
無線
トランシーバ
回路
34
モードセレクタ
比較器
32
ハンドオーバー
利用性
決定装置
36
28
118
28"
22
中央制御
ユニット
24
外部通信ネットワーク
バックボーン
38
AP
リスト
1. AP #
n. AP#
14
18
12
移動
ターミナル
28'

FIG. 1

【図２】

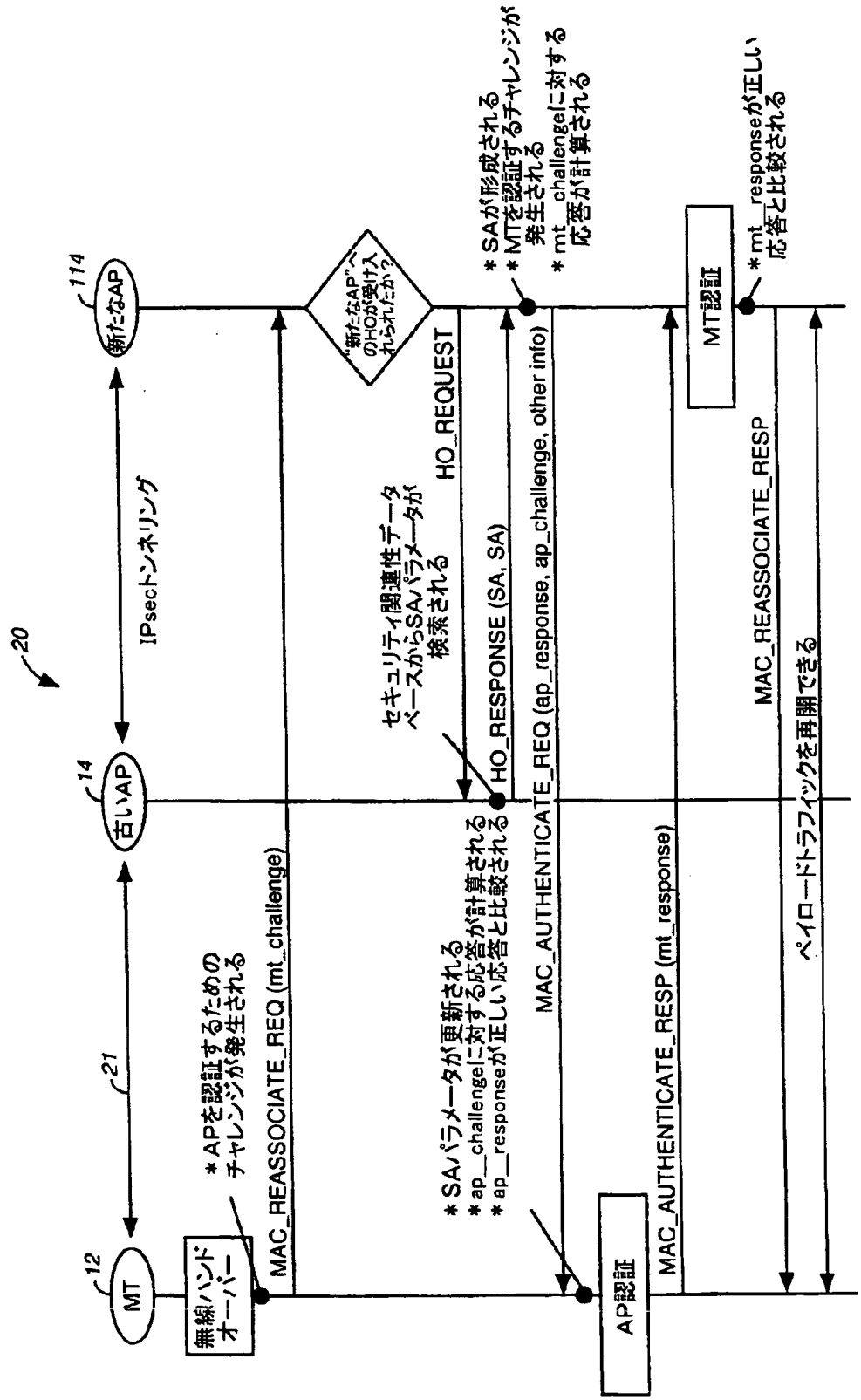

20
IPsecトンネリング
114
新たなAP
14
古いAP
12
MT
21
無線ハンドオーバー
"新たなAP"へのHOが受け入れられたか？
HO_REQUEST
セキュリティ関連性データベースからSAパラメータが検索される
HO_RESPONSE (SA, SA)
＊SAが形成される
＊MTを認証するチャレンジが発生される
＊mt_challengeに対する応答が計算される
MT認証
＊mt_responseが正しい応答と比較される
MAC_REASSOCIATE_RESP
＊APを認証するためのチャレンジが発生される
MAC_REASSOCIATE_REQ (mt_challenge)
＊SAパラメータが更新される
＊ap_challengeに対する応答が計算される
＊ap_responseが正しい応答と比較される
MAC_AUTHENTICATE_REQ (ap_response, ap_challenge, other info)
AP認証
MAC_AUTHENTICATE_RESP (mt_response)
ペイロードトラフィックを再開できる

FIG. 2

【図３】

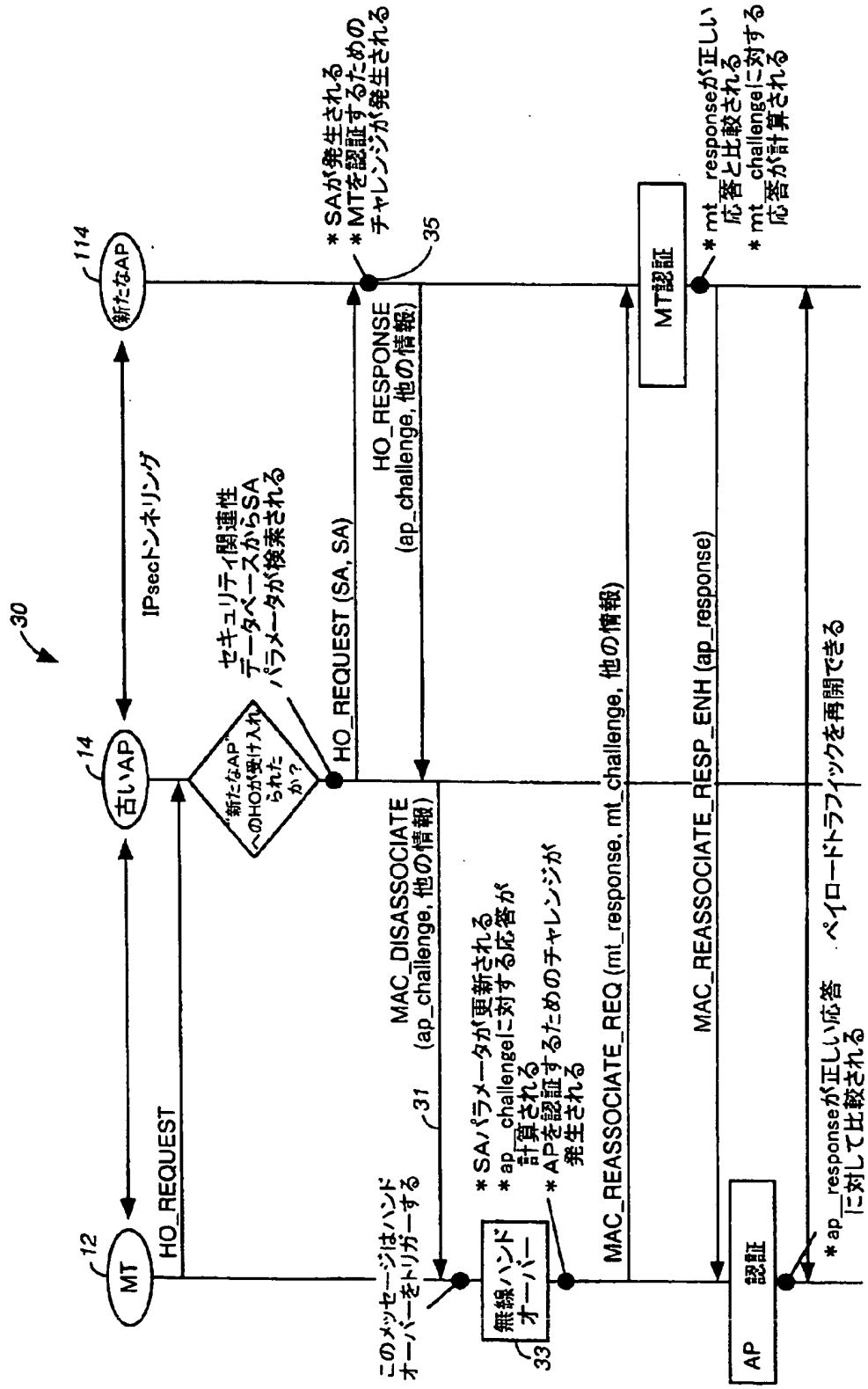

30
MT
12
古いAP
14
新たなAP
114
IPsecトンネリング
HO_REQUEST
このメッセージはハンドオーバーをトリガーする
新たなAPへのHOが受け入れられたか？
セキュリティ関連性データベースからSAパラメータが検索される
HO_REQUEST (SA, SA)
* SAが発生される
* MTを認証するためのチャレンジが発生される
35
HO_RESPONSE (ap_challenge, 他の情報)
MAC_DISASSOCIATE (ap_challenge, 他の情報)
31
無線ハンドオーバー
33
* SAパラメータが更新される
* ap_challengeに対する応答が計算される
* APを認証するためのチャレンジが発生される
MAC_REASSOCIATE_REQ (mt_response, mt_challenge, 他の情報)
MT認証
MAC_REASSOCIATE_RESP_ENH (ap_response)
* mt_responseが正しい応答と比較される
* mt_challengeに対する応答が計算される
AP認証
* ap_responseが正しい応答に対して比較される
ペイロードトラフィックを再開できる

FIG. 3

【図４Ａ】

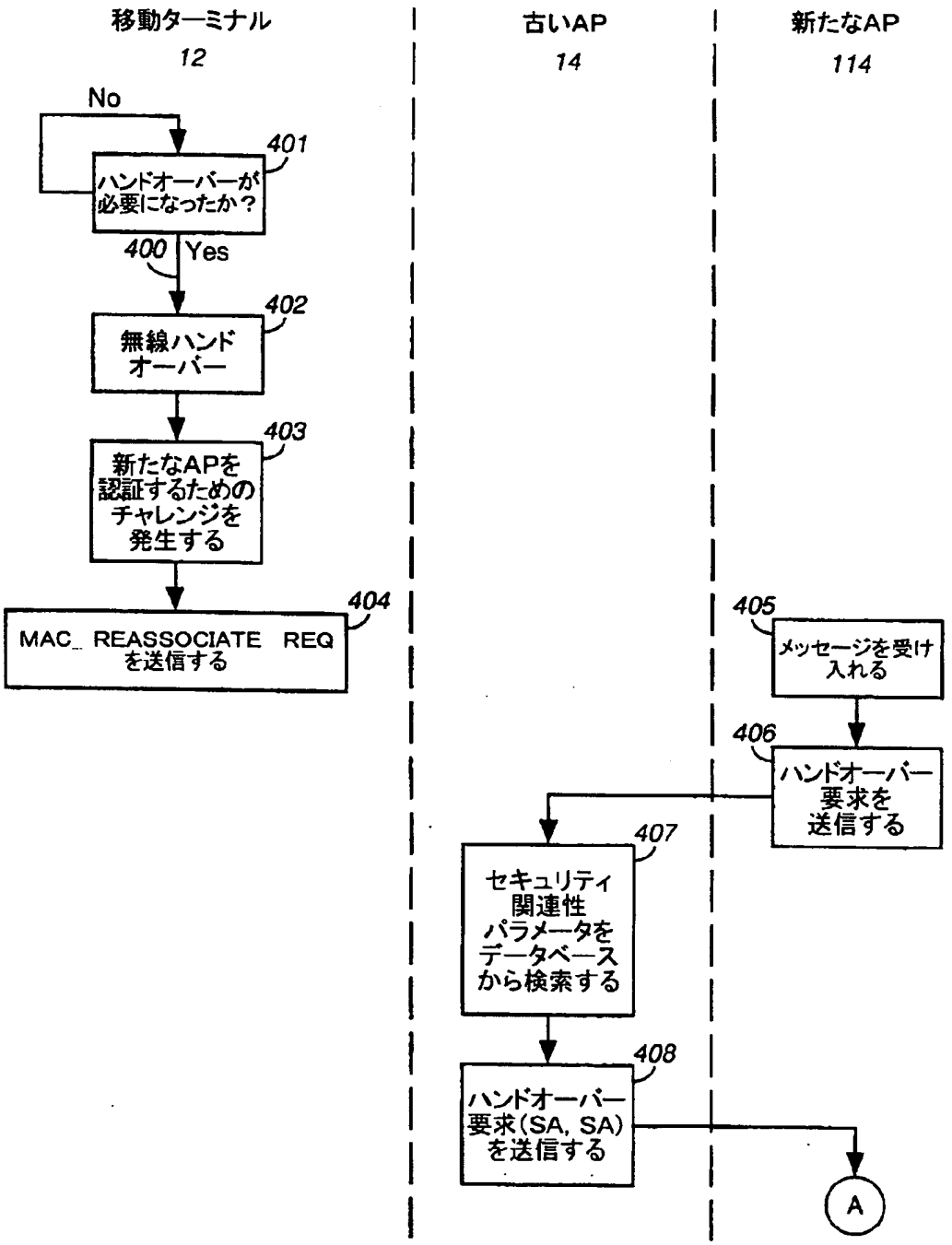

移動ターミナル
12
古いAP
14
新たなAP
114
No
401
ハンドオーバーが必要になったか？
400
Yes
402
無線ハンドオーバー
403
新たなAPを認証するためのチャレンジを発生する
404
MAC_ REASSOCIATE REQ を送信する
405
メッセージを受け入れる
406
ハンドオーバー要求を送信する
407
セキュリティ関連性パラメータをデータベースから検索する
408
ハンドオーバー要求(SA, SA)を送信する
A

FIG. 4A

【図４Ｂ】

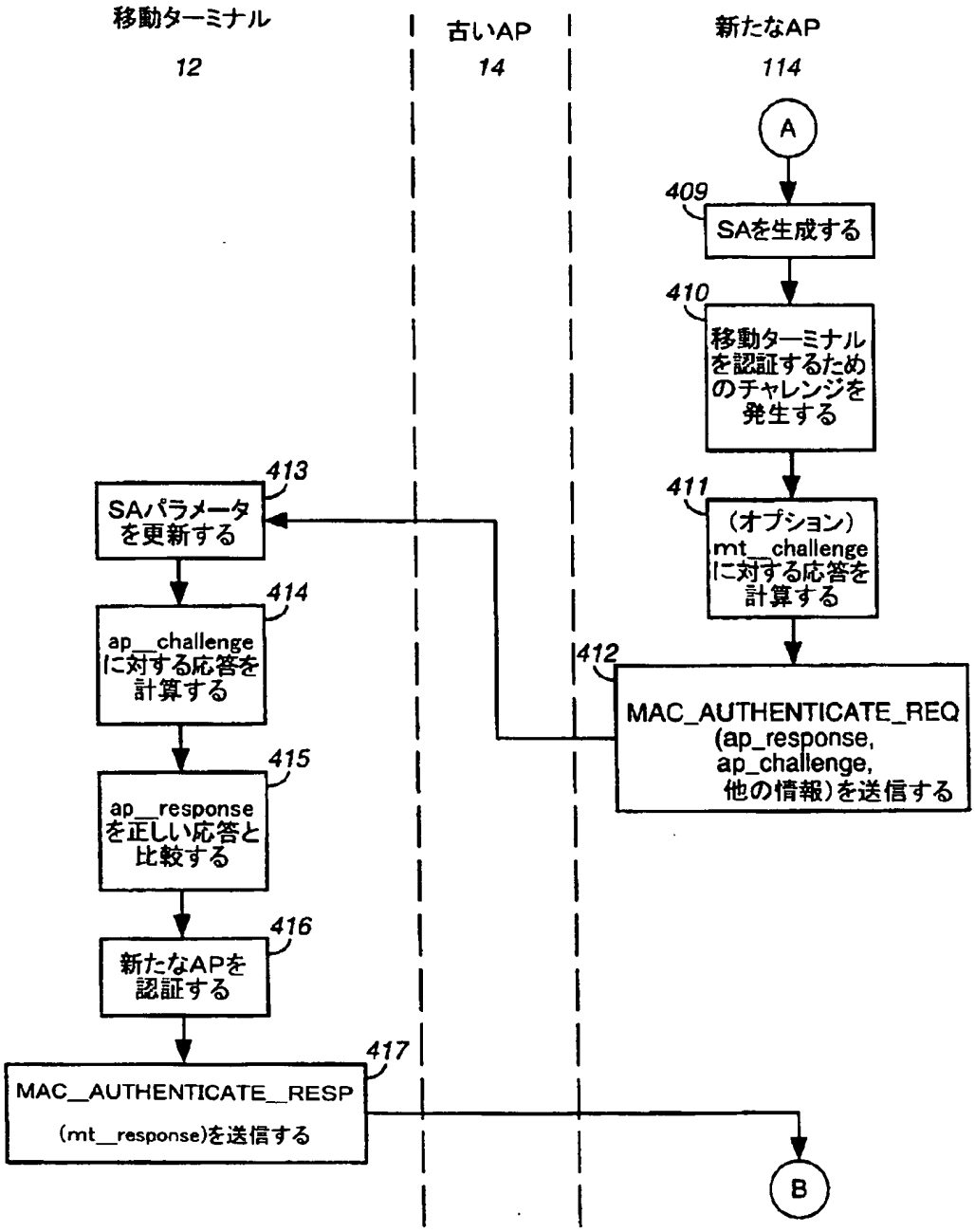

移動ターミナル
12
古いAP
14
新たなAP
114
A
409
SAを生成する
410
移動ターミナルを認証するためのチャレンジを発生する
411
(オプション) mt__challengeに対する応答を計算する
412
MAC_AUTHENTICATE_REQ (ap_response, ap_challenge, 他の情報)を送信する
413
SAパラメータを更新する
414
ap__challengeに対する応答を計算する
415
ap__responseを正しい応答と比較する
416
新たなAPを認証する
417
MAC__AUTHENTICATE__RESP (mt__response)を送信する
B

FIG. 4B

【図４Ｃ】

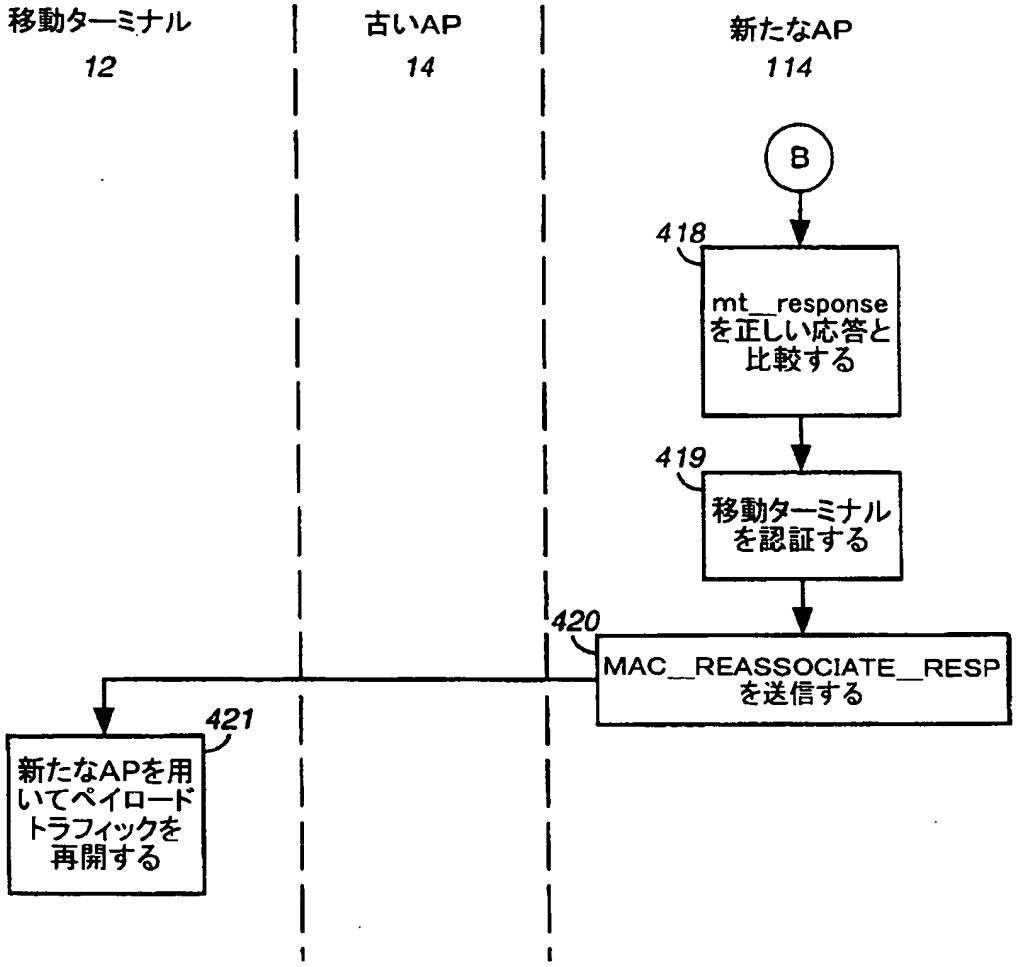

移動ターミナル
12
古いAP
14
新たなAP
114
B
418
mt_response
を正しい応答と
比較する
419
移動ターミナル
を認証する
420
MAC_REASSOCIATE_RESP
を送信する
421
新たなAPを用
いてペイロード
トラフィックを
再開する

FIG. 4C

【図５Ａ】

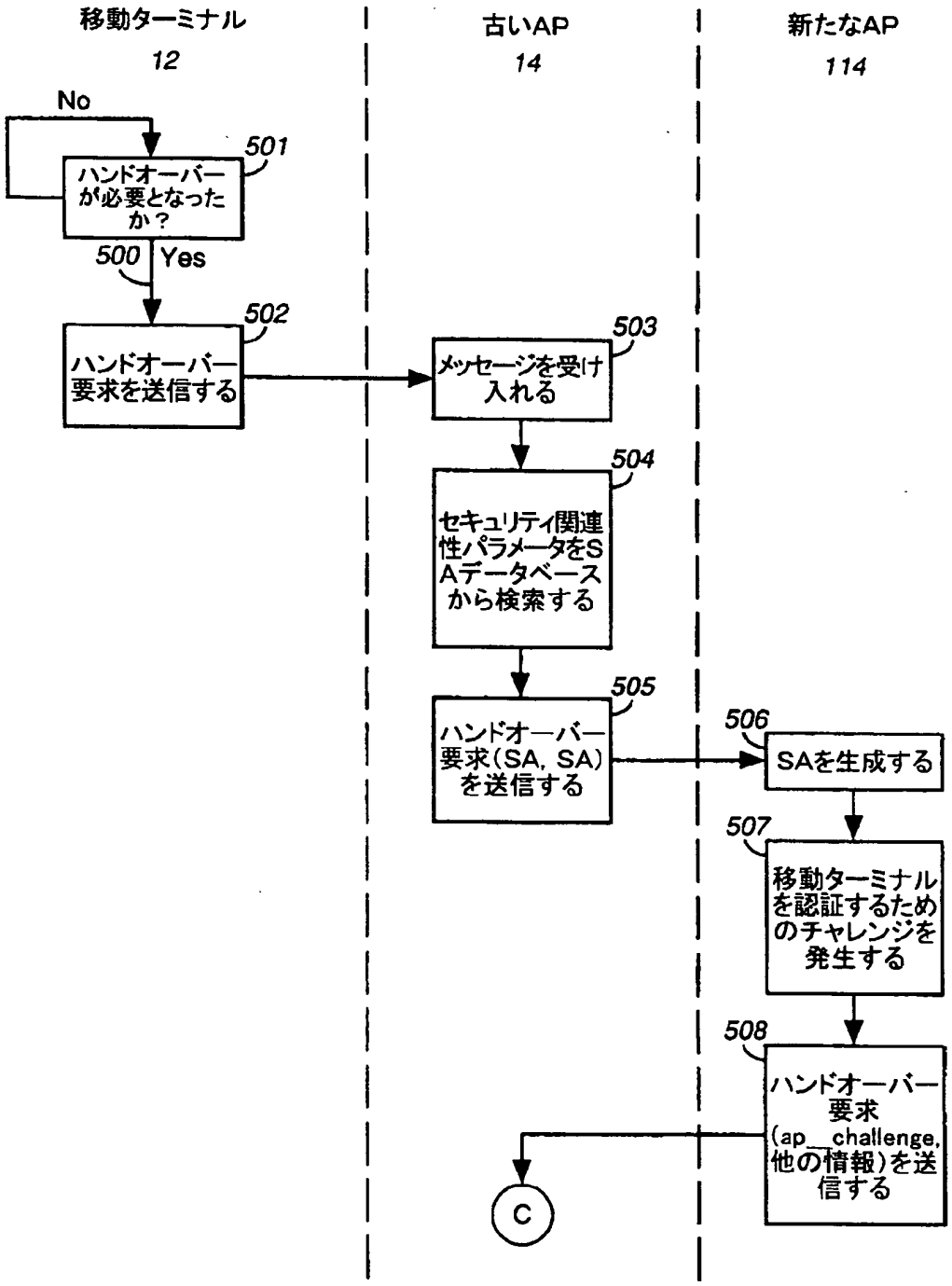

移動ターミナル
12
古いAP
14
新たなAP
114
No
501
ハンドオーバーが必要となったか？
500
Yes
502
ハンドオーバー要求を送信する
503
メッセージを受け入れる
504
セキュリティ関連性パラメータをSAデータベースから検索する
505
ハンドオーバー要求(SA, SA)を送信する
506
SAを生成する
507
移動ターミナルを認証するためのチャレンジを発生する
508
ハンドオーバー要求(ap_challenge, 他の情報)を送信する
C

FIG. 5A

【図５Ｂ】

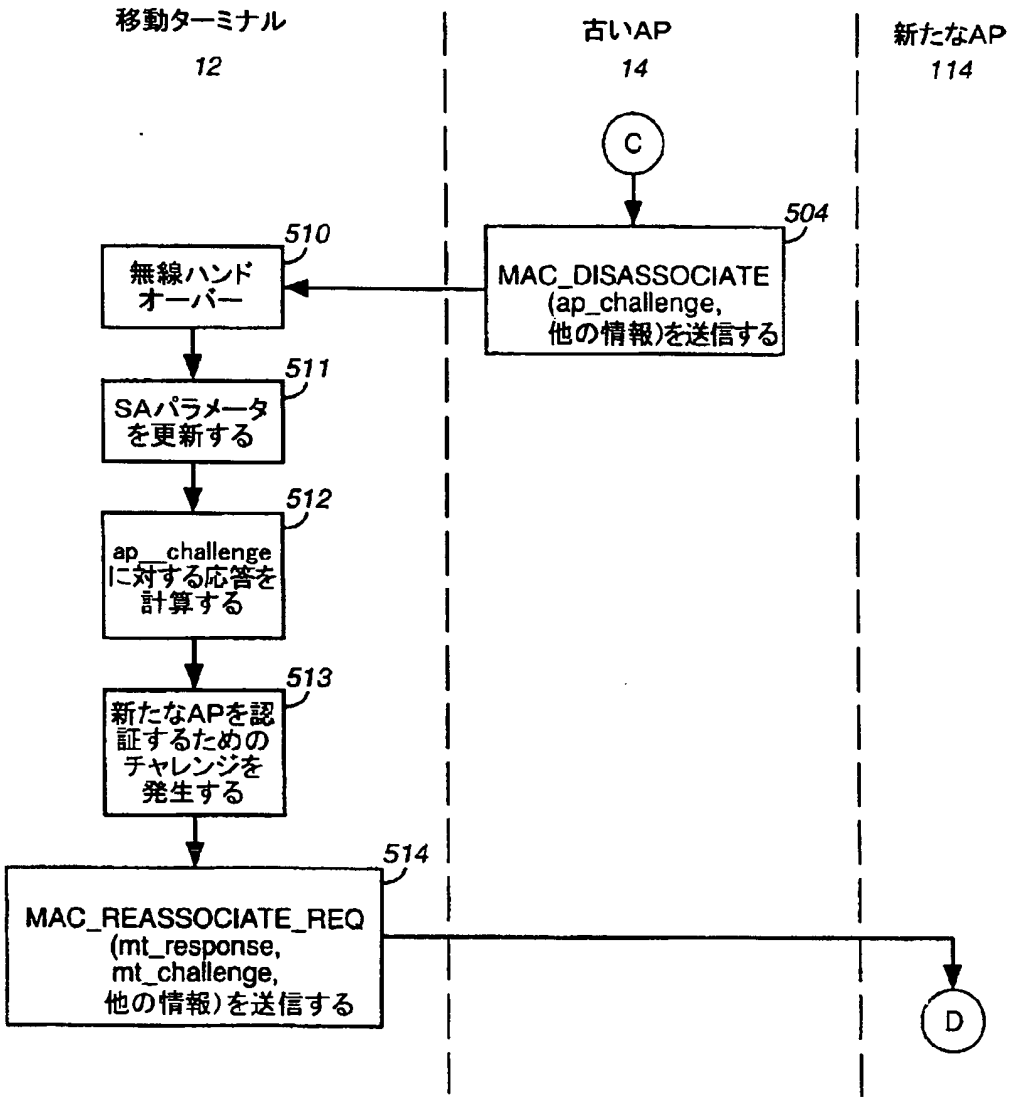

移動ターミナル
12
古いAP
14
新たなAP
114
C
504
MAC_DISASSOCIATE
(ap_challenge,
他の情報)を送信する
510
無線ハンド
オーバー
511
SAパラメータ
を更新する
512
ap__challenge
に対する応答を
計算する
513
新たなAPを認
証するための
チャレンジを
発生する
514
MAC_REASSOCIATE_REQ
(mt_response,
mt_challenge,
他の情報)を送信する
D

FIG. 5B

【図５Ｃ】

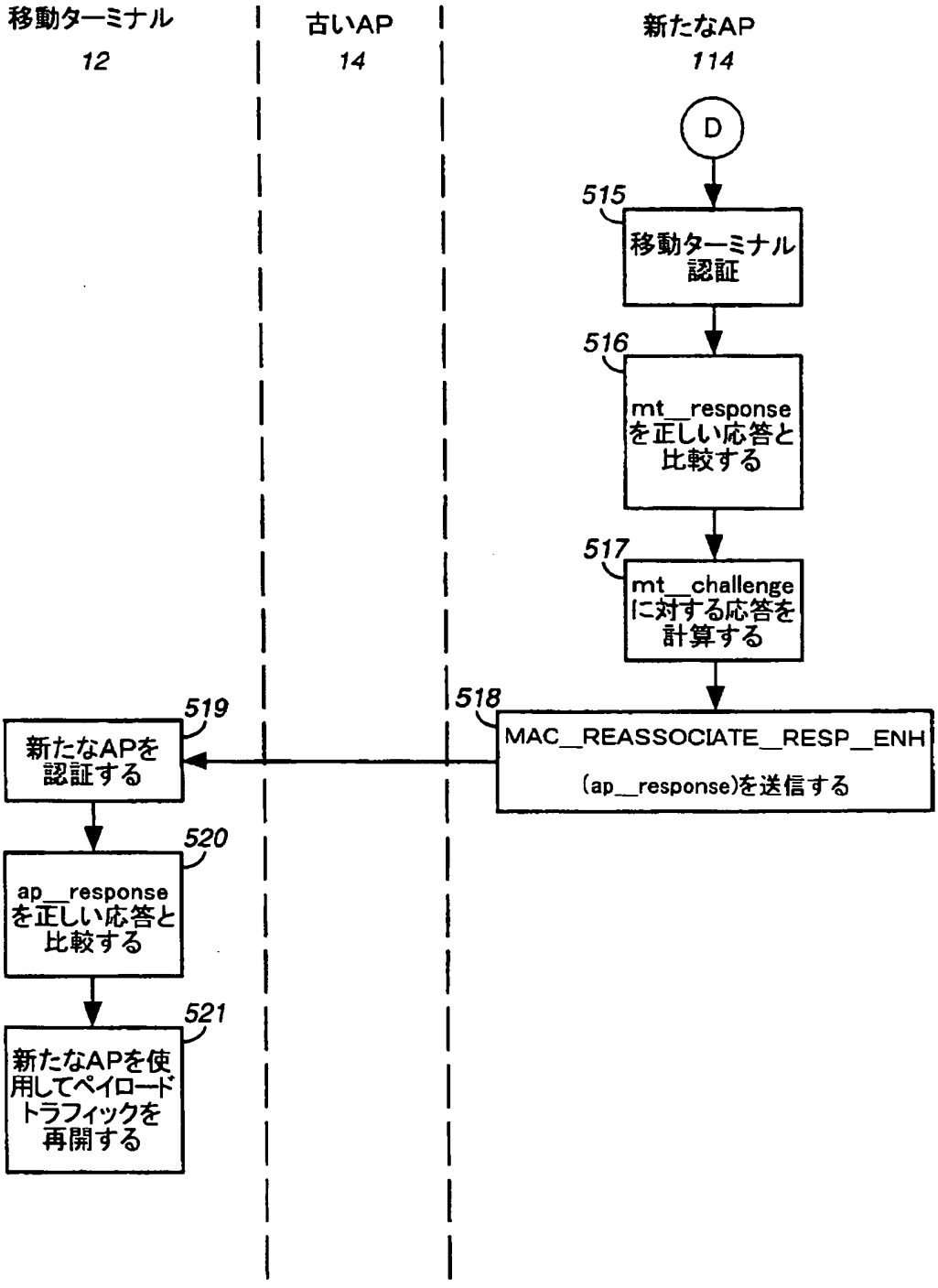

移動ターミナル
12
古いAP
14
新たなAP
114
D
515
移動ターミナル認証
516
mt__responseを正しい応答と比較する
517
mt__challengeに対する応答を計算する
518
MAC__REASSOCIATE__RESP__ENH
(ap__response)を送信する
519
新たなAPを認証する
520
ap__responseを正しい応答と比較する
521
新たなAPを使用してペイロードトラフィックを再開する

FIG. 5C

【図６】

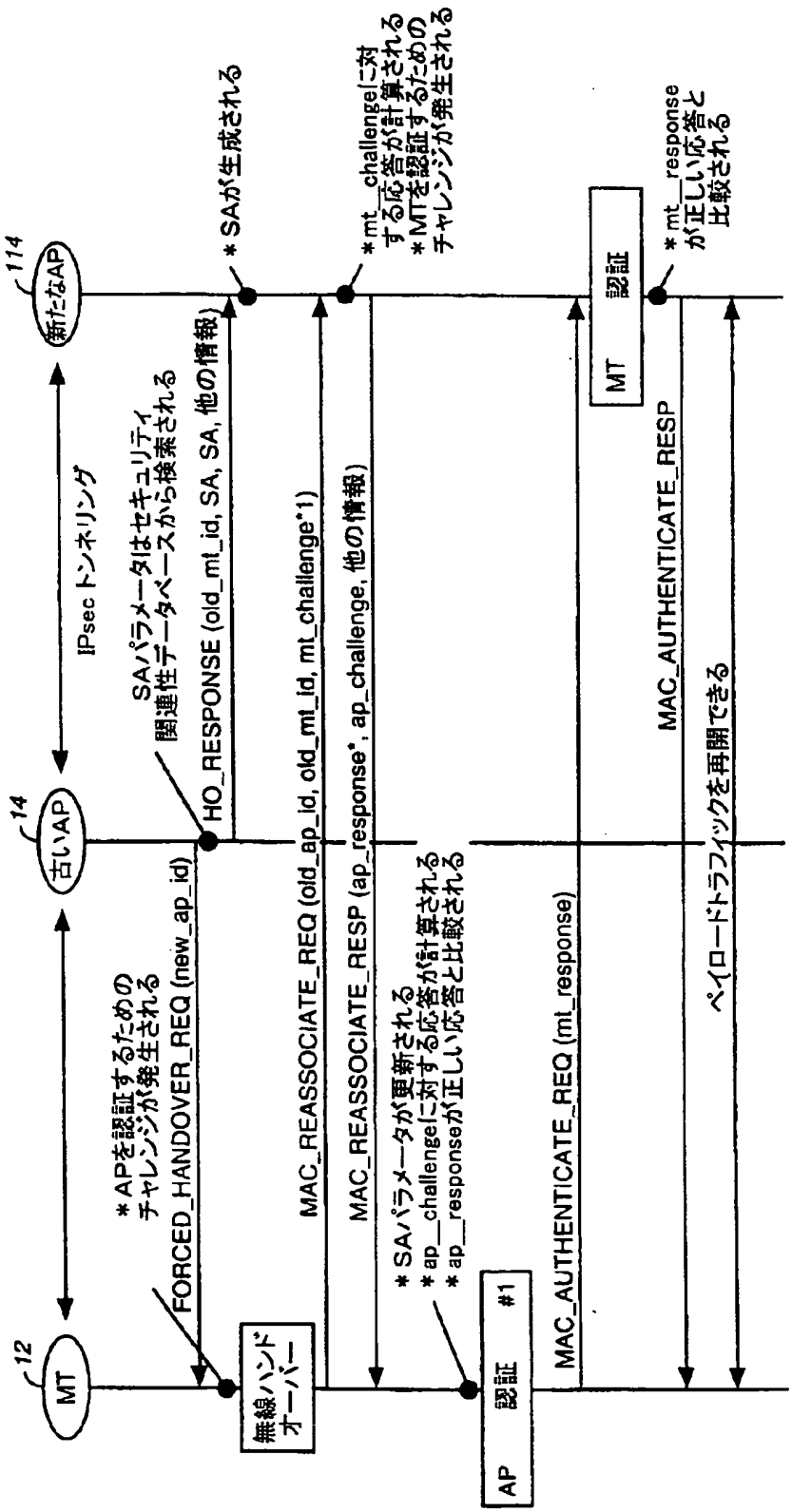

12
MT
14
古いAP
114
新たなAP
無線ハンドオーバー
AP 認証 #1
MT 認証
IPsec トンネリング
SAパラメータはセキュリティ関連性データベースから検索される
＊APを認証するためのチャレンジが発生される
FORCED_HANDOVER_REQ (new_ap_id)
HO_RESPONSE (old_mt_id, SA, SA, 他の情報)
＊SAが生成される
MAC_REASSOCIATE_REQ (old_ap_id, old_mt_id, mt_challenge*1)
MAC_REASSOCIATE_RESP (ap_response*, ap_challenge, 他の情報)
＊SAパラメータが更新される
＊ap__challengeに対する応答が計算される
＊ap__responseが正しい応答と比較される
＊mt__challengeに対する応答が計算される
＊MTを認証するためのチャレンジが発生される
MAC_AUTHENTICATE_REQ (mt_response)
MAC_AUTHENTICATE_RESP
＊mt__responseが正しい応答と比較される
ペイロードトラフィックを再開できる

FIG. 6

【図７】

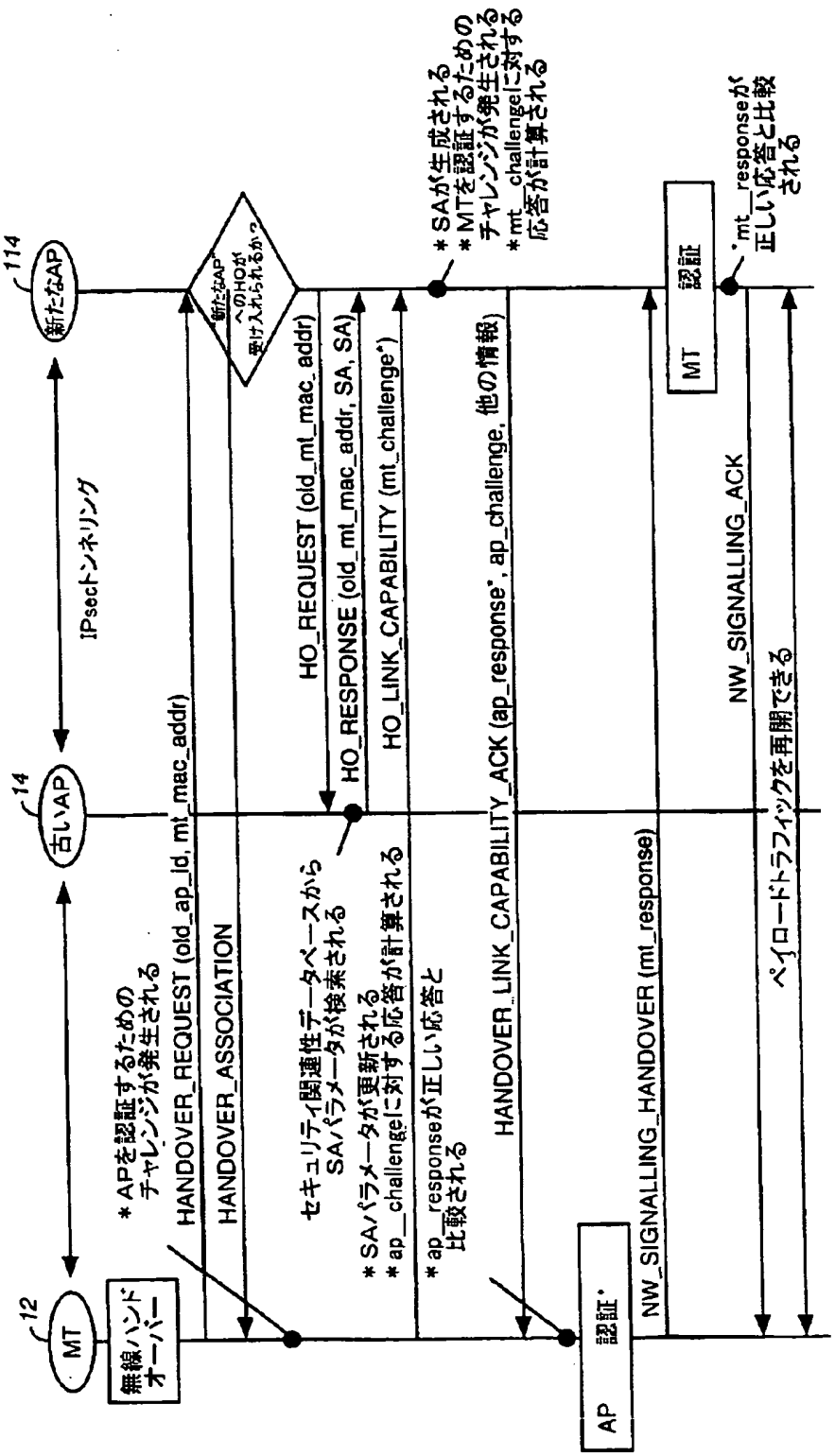

MT
無線ハンドオーバー
古いAP
新たなAP
IPsecトンネリング
＊APを認証するためのチャレンジが発生される
HANDOVER_REQUEST (old_ap_Id, mt_mac_addr)
HANDOVER_ASSOCIATION
新たなAPへのHOが受け入れられるか？
セキュリティ関連性データベースからSAパラメータが検索される
＊SAパラメータが更新される
＊ap_challengeに対する応答が計算される
HO_REQUEST (old_mt_mac_addr)
HO_RESPONSE (old_mt_mac_addr, SA, SA)
HO_LINK_CAPABILITY (mt_challenge')
＊ap_responseが正しい応答と比較される
＊SAが生成される
＊MTを認証するためのチャレンジが発生される
＊mt_challengeに対する応答が計算される
HANDOVER_LINK_CAPABILITY_ACK (ap_response', ap_challenge, 他の情報)
AP 認証'
NW_SIGNALLING_HANDOVER (mt_response)
MT 認証
'mt_responseが正しい応答と比較される
NW_SIGNALLING_ACK
ペイロードトラフィックを再開できる

FIG. 7

【手続補正書】特許協力条約第３４条補正の翻訳文提出書

【提出日】平成１３年１０月９日（２００１．１０．９）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項１】　所定の移動ターミナル(12)との通信が第１アクセスポイント(14)から第２アクセスポイント(114)へハンドオーバーされるときに情報セキュリティを与える方法(20)において、

複数のアクセスポイント(14,114)を有する通信システム(10)を用意し、各アクセスポイントは、上記通信システムによりサービスされる全地理的エリア内の異なる地理的エリア(18,118)にサービスし、

上記全地理的エリア内で上記異なる地理的エリア(18,118)間を各々物理的に移動可能な複数の移動ターミナル(12)を用意し、

上記所定の移動ターミナルが上記第１アクセスポイントとの通信作用から上記第２アクセスポイントとの通信作用へ移動するときを感知し(401)、

上記感知段階に応答して、上記第１アクセスポイント(14)からセキュリティ関連性パラメータを検索し(407)、その検索されたセキュリティ関連性パラメータに基づき上記第２アクセスポイント(114)にセキュリティ関連性を形成し(409)、そしてその検索されたセキュリティ関連性パラメータに基づいて上記所定の移動ターミナル(12)にセキュリティ関連性を形成し、そして

上記応答段階に基づいて上記所定の移動ターミナル(12)と上記第２アクセスポイント(114)との間に通信を開始する(421)、

という段階を備えた方法。

【請求項２】　上記の感知段階(401)に応答して、上記所定の移動ターミナル(12)から上記第２アクセスポイント(114)へ認証アクセスポイントチャレンジ(412)を送信し(404)、そして上記第２アクセスポイント(114)から上記所定の移動

ターミナル(12)へ認証移動ターミナルチャレンジを送信し(412)、

上記所定の移動ターミナル(12)から受け取った上記認証アクセスポイントチャレンジに応答して上記第２アクセスポイント(114)に認証アクセスポイント応答を発生し(410)、

上記認証アクセスポイント応答を上記所定の移動ターミナルへ送信し(412)、

上記第２アクセスポイントから受け取った上記認証移動ターミナルチャレンジに応答して上記所定の移動ターミナル(12)に認証移動ターミナル応答を発生し(414)、

上記認証移動ターミナル応答を上記第２アクセスポイントへ送信し(417)、

上記認証アクセスポイント応答を上記所定の移動ターミナルにおいて正しい応答と第１比較し(415)、

上記認証移動ターミナル応答を上記第２アクセスポイントにおいて正しい応答と第２比較し(418)、そして

上記第１比較段階及び上記第２比較段階に基づいて上記所定の移動ターミナルと上記第２アクセスポイントとの間に通信を開始する(420)、

段階を更に備えた請求項１に記載の方法(20)。

【請求項３】　上記複数の移動ターミナル(12)は、媒体アクセス制御層及び互換性物理層を有し、そして上記メッセージは、媒体アクセス制御メッセージである請求項２に記載の方法(20)。

【請求項４】　上記メッセージは、ワイヤレスＬＡＮ内に送信され、ＩＥＥＥ８０２．１１又はＨＩＰＥＲＬＡＮ／２マルチアクセスメッセージである請求項３に記載の方法(20)。

【請求項５】　上記通信システム(10)は、セキュリティプロトコルを使用してデータパケットの端－端セキュリティを与えるＷＬＡＮ通信システムである請求項２に記載の方法(20)。

【請求項６】　上記端－端セキュリティは、上記データパケットを認証及び／又は暗号化することにより与えられ、そして上記セキュリティプロトコルは、通信リンクの両端で同じ暗号及び／又は認証キーの使用を必要とする対称的暗号を与える請求項５に記載の方法(20)。

【請求項７】　シール可能なキー管理プロトコルは、上記セキュリティプロトコルに対する対称的キーを発生するよう動作する請求項６に記載の方法(20)。

【請求項８】　上記所定の移動ターミナルと上記第２のアクセスポイントとの間にセッション従属動的暗号化キーを与え、そして

上記通信システムにより与えられる通信カバレージ内で上記所定の移動ターミナルが移動するときに第１アクセスポイントから第２アクセスポイントへアクティブなセキュリティ関連性を転送する、

という段階を備えた請求項６に記載の方法(20)。

【請求項９】　上記通信システム(10)をＬＡＮとして用意し、

上記ＬＡＮ内にサーバーを用意し、

通信ハンドオーバー中に通信が続くときに、端－端セキュリティ関連性に変更を必要とせずに、通信ハンドオーバー中に上記ＬＡＮ内にキー管理及びセキュリティ関連性再確立を与え、上記通信ハンドオーバーが上記移動ターミナルと上記第１及び第２アクセスポイントとの間のセキュリティ機能にしか影響しないようにする、

という段階を備えた請求項４に記載の方法(20)。

【請求項１０】　上記ＬＡＮは、上記複数のアクセスポイント(14, 114)と上記複数の移動ターミナル(12)との間にインターネットプロトコルセキュリティベースのセキュリティ関連性を含む請求項９に記載の方法(20)。

【請求項１１】　上記所定の移動ターミナル(12)及び上記第１及び第２のアクセスポイント(14, 114)で作られた通信対の両端に対して認証キーが与えられ、この認証キーは、スケーリング可能なキー管理プロトコルにより発生される請求項１に記載の方法(20)。

【請求項１２】　上記所定の移動ターミナル(12)と上記第１アクセスポイント(14)との間にはスケーリング可能なキー管理プロトコルに基づいて認証キー又はセキュリティ関連性が存在し、そして通信ハンドオーバー中に新たなキー交換の必要性を回避するために上記複数のアクセスポイント(14, 114)間にセキュリティ関連性が転送される請求項１に記載の方法(20)。

【請求項１３】　上記スケーリング可能なキー管理プロトコルは、ＩＫＥで

あり、そして上記第１アクセスポイント(14)から上記第２アクセスポイント(114)への上記通信ハンドオーバー中に新たなキー交換の必要性を回避するやり方で上記第１アクセスポイント(14)と上記第２アクセスポイント(114)との間にセキュリティ関連性が転送される請求項１２に記載の方法(20)。

【請求項１４】　キーを搬送するメッセージを暗号化する段階を含む請求項１３に記載の方法(20)。

【請求項１５】　第１通信アクセスポイント(14)によりサービスされる第１地理的エリア(18)から、第２通信アクセスポイント(114)によりサービスされる第２地理的エリア(118)へ移動ターミナル(12)が物理的に移動するときに通信ハンドオーバーが発生するとき無線通信システム(10)に所定のセキュリティ関連性を維持するための装置であって、上記移動ターミナル(12)は、最初に、上記第１通信アクセスポイント(14)と第１通信対を形成し、そして上記通信ハンドオーバーの後に、上記移動ターミナルは、上記第２通信アクセスポイント(114)と第２通信対を形成し、上記第１通信対(12-14)の各メンバーは、それに関連した上記所定のセキュリティ関連性を有し、上記装置は、

上記移動ターミナル(12)にあって上記通信ハンドオーバーを開始する必要性を感知するための第１手段(40)と、

上記無線通信システム(10)内にあって、上記第１手段(40)が上記通信ハンドオーバーを開始する上記必要性を感知するのに応答して、上記第２通信アクセスポイント(114)に上記所定のセキュリティ関連性を確立するための第２手段(405)と、

上記移動ターミナル(12)にあって、上記所定のセキュリティ関連性の関数としてアクセスポイントチャレンジを発生し、そしてそのアクセスポイントチャレンジを上記第２通信アクセスポイントへ送信するための第３手段(403)と、

上記第２通信アクセスポイントにあって、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として移動ターミナルチャレンジを発生し、そしてその移動ターミナルチャレンジを上記移動ターミナルへ送信するための第４手段(410)と、

上記移動ターミナルにあって、上記移動ターミナルチャレンジに応答して、上

記所定のセキュリティ関連性の関数として移動ターミナル応答を発生し、そしてその移動ターミナル応答を上記第２通信アクセスポイントへ送信するための第５手段(414)と、

上記第２通信アクセスポイントにあって、上記アクセスポイントチャレンジに応答して、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数としてアクセスポイント応答を発生し、そしてそのアクセスポイント応答を上記移動ターミナルへ送信するための第６手段(409)と、

上記移動ターミナルにあって、上記アクセスポイント応答に応答して、上記アクセスポイント応答が上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第７手段と、

上記第２通信アクセスポイント(114)にあって、上記移動ターミナル応答に応答して、上記移動ターミナル応答が、上記第２通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第８手段(418)と、

上記無線通信システム(10)内にあって、上記第８及び第９手段に応答して、上記移動ターミナル応答及び上記アクセスポイント応答の両方が正しいときに上記通信ハンドオーバーを確立するための第９手段(420)と、

を備えた装置。

【請求項１６】　上記無線通信システム(10)は、グループＩＥＥＥ８０２．１１及びＨＩＰＥＲＬＡＮから選択される請求項１５に記載の装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intern. ial Application No
PCT/IB 00/01713

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 939 519 A (NO WIRES NEEDED B V) 1 September 1999 (1999-09-01) column 4, line 8 - line 58 figure 1	15,18,20
A	US 5 778 075 A (HAARTSEN JACOBUS CORNELIS) 7 July 1998 (1998-07-07) column 4, line 24 - line 50 column 9, line 43 - line 60 column 18, line 15 - line 60 figures 5,13	1
P,X	WO 00 49827 A (ERICSSON TELEFON AB L M) 24 August 2000 (2000-08-24) page 2, line 20 -page 5, line 25 figure 2	1

☐ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the an which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 April 2001	11/04/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Barel, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. al Application No
PCT/IB 00/01713

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0939519	A	01-09-1999	NL	1008351 C	20-08-1999
US 5778075	A	07-07-1998	AU	3875797 A	19-03-1998
			WO	9809458 A	05-03-1998
			SE	9900589 A	07-05-1999
WO 0049827	A	24-08-2000	AU	2954300 A	04-09-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者 サルヴェラ ユハ
フィンランド エフイーエン－02150 エスプー オタカリオ １セ28

Ｆターム(参考) 5K033 AA08 CB14 DA19
5K067 AA30 BB04 DD11 DD17 DD36 EE02 EE10 EE24 HH01 JJ71 JJ78